Editors

Niculae IANCU

Irena DUMITRU

INTELLIGENCE IN THE KNOWLEDGE SOCIETY

Proceedings of the XIXth International Conference

EDITURA ANIMV

Bucharest – 2014

Editura Academiei Naţionale de Informaţii *„Mihai Viteazul”*
Telefon: 021 4106550/1186,1204,1172
Fax: 0213104714

COLECTIVUL DE REDACŢIE

Redactor şef:	Valentin NICULA
Redactori:	Teodora DOBRE Valentin STOIAN
Tehnoredactare:	Alexandra VIZITIU
Coperta:	Valentin NICULA

Bun de tipar:07.10.2014 Apărut: octombrie 2014
Tipărit sub comanda nr. NS8971611/06.10.2014.

EDITURA
ANIMV

ISSN 2392 – 7542

PROCEEDINGS
# of the XIXth International Conference
INTELLIGENCE IN THE KNOWLEDGE SOCIETY 2013
TABLE OF CONTENTS

Intelligence Tradecraft in the Knowledge Society

New Challenges, Evolving Threats

Tools and Methods for Intelligence Theory and Practice

Integrating Different Perspectives on Intelligence

Foreword

"...all attempts to develop ambitious theories of intelligence have failed" - *Walter Laqueur*[1]

We have witnessed in the last decades a fast growth in the number of intelligence training and research programs across Europe and beyond. This is a clear indicator of the raised awareness of both ordinary citizens and decision-makers on the importance of structuring academically the debate on security and the role of intelligence agencies.

Nevertheless, as things change, the more they stay the same. Some of the key questions intelligence experts are asking today are by no means new. What is intelligence? What does just practice in intelligence mean - are queries which have been the focus of studies and analyses since the very creation of this field. For example, finding a widely accepted definition for intelligence is proving to be slippery, as this may entail a rethinking of the core theoretical framework, with significant scientific and policy implications.

On the other hand the continuously evolving security environment makes security and intelligence anxious of their foresight ability so as to preserve their competitiveness on a very dynamic information market. The role of intelligence for decision-making is challenged as never before, as open source information multiply and the evolution of communication means makes it almost impossible to control information dissemination.

That is why having a forum where experts can both openly debate on current security issues and dwell on longstanding academic controversies is sorely needed.

The Intelligence in the Knowledge Society International Conference (IKS) taking place every autumn in Bucharest tries to bridge the gap between researchers and practitioners, building confidence and establishing partnerships.

Though Romania's visibility in this field has gradually increased over the years, with its participation in various research and cooperation networks, it still has many challenges ahead.

However, the IKS' versatility in both composition of participants and topics to be addressed makes it an internationally sought event.

[1] Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York, NY: Basic Books, 1985), p. 8.

The 2013 edition benefited from the participation of high level decision-makers, experienced practitioners coming from various intelligence agencies, both inside and outside Europe and many active researchers in the field of intelligence and security studies.

As we move further away from the traditional intelligence paradigm, which has shown to be inefficient in addressing the new transnational and global threat to security, experts are trying to design a more creative and collaborative intelligence process, which would enable intelligence organizations to become more dynamic and interconnected.

Academic events, such as the IKS Conference are places where previous assumptions are being questioned by experts who do not necessarily share the same background, training, or nationality, leading to a better understanding of security issues.

The main topics on the 2013 conference agenda were: *strategic foresight, cyber security, social media, intelligence culture, intelligence analysis and intelligence sharing*. The debates were focused on means to bring intelligence studies closer to other social disciplines in an effort to enrich the knowledge shared by practitioners. The question of the hour was ”How to make our intelligence services better” outside of the limits previously imposed by the secrecy paradigm. Though, no consensus has been reached, the discussion opened up many pathways that could and will be explored in future events. This goes to show that many times the solutions for the key intelligence problems are not to be found solely in the people holding security clearances but they may be provided by people outside the intelligence community, coming from the academia, business sector or civil society.

This volume integrates some of the valuable academic papers presented during the conference and is one of the steps we are undertaking in sharing some of valuable expertise which is to be found in Romania and elsewhere. It is also an important step towards building a security and intelligence culture in Romania, while at the same time contributing to an improved understanding of the role and place of intelligence in democratic societies.

That is why we dedicated this book not only to intelligence practitioners, but also to researchers, decision-makers and ordinary citizens who may be interested in learning more on the complexities and challenges of security and intelligence field.

The editors

All Source Intelligence Tradecraft: a Multidisciplinary Perspective

Michael ANDREGG[*]

Abstract

The world faces extraordinary challenges today that perplex even the largest and richest intelligence agencies. Interdisciplinary problems with small military dimensions but large security consequences abound, like global climate change, terrorism and cyber-war, transnational crime (including financial crimes by nominally reputable corporations) and flows of refugees from failed and failing states. This ***"developing global crisis"*** *forces official intelligence agencies to rely ever more on liaisons with other agencies, and with academics, NGOs or other members of polite society. But there are "culture chasms" between these worlds that make effective liaison difficult. This paper explores those dimensions and core values of scholars and spies, then provides a long list of partial solutions including: 1) a porous security barrier, 2) a spirit of ecumenism, 3) better public diplomacy and strategic culture, 4) respect for both long and short term priorities, 5) less bureaucracy and more sharing, 6) reducing institutional roadblocks to change, 7) more collaborations on common problems, 8) and a focus on corruption of governance as a key transnational problem (even though that is especially risky for official agencies and agents to study).*

The paper ends with a few words about the interdisciplinary future and global intelligence enterprise.

Keywords: global intelligence enterprise, culture chasms crisis, emerging threats, liaisons

Introduction

"80% or more of what you need to know can be found in open sources" - That was a truism of analytic tradecraft 30 years ago. Modern information technologies make it even truer today[1]. Search engines can now bring more data in seconds than anyone could synthesize in months, much less validate or fact check, and most analysts do not have months to finish their missions. They are lucky if they have days. The power of the new technologies has encouraged the rise of a new kind of "information professional" the OSINT specialist (Open Source Intelligence). Yet, what analysts, operators and leaders really need to know in a crisis often remains elusive.

[*] Ph.D. geneticist with unusual access to intelligence professionals of all types from many countries, d-final, USA

One obvious reason for this is that the dangerous men and institutions that intelligence agencies are most curious about work hard to preserve their secrets. They are unlikely to post travel plans on Facebook or tweet reactions to world events to a crowd of anonymous followers. Less obvious, but no less important, the internet is dominated by English language material that is over a year old. Most intelligence taskings are for current conditions in regions where English is associated with colonial interests. The best material for those problems generally will not be in English and will not be posted on the internet anytime soon.

So security agencies often fall back on the tried and true techniques of human intelligence (HUMINT) and wiretaps or other signals intelligence (SIGINT). They try to put a spy or a wire on the targets of their curiosity. Such sources and methods are very vulnerable if discovered (spies can be killed or fed false information, and phone lines once known to be compromised are seldom used again). Thus protecting sources and methods becomes a universal priority among intelligence agencies.

Enter the subject matter expert (SME) who is not a spy, but more likely a professor, a journalist or sometimes clergy or other professional, who has spent years learning about a rare topic like the Pashtun people's worldview or nuclear physics in North Korea that has become important to an intelligence agency. A true "all sources" assessment benefits from combining secrets gleaned from human sources and communications interceptions, both of which need protection, with the expertize of the SME. Problem is, many SMEs won't cooperate with spy agencies for a long list of excellent reasons beginning with the security clearance barrier. A prime goal of this paper is a detailed review of why that is and partial ways to get around it. One thing we know for sure: there is no perfect or easy way around this culture chasm.

Historic Antecedents and the Current Crisis

Spies have collaborated with intellectuals since the beginning of recorded history when distinctions like that were less bureaucratized. Sun Tzu devotes an entire chapter of his classic

"Art of War" to the management of spies, and stresses among other things the subtlety required to recruit the "most intelligent" and best placed agents inside an enemy's court or military staff[2]. For decades, the CIA was staffed mainly by graduates of Princeton, Yale, Harvard and a few other "ivy league" colleges along with military veterans from its predecessor OSS. The veterans were generally better at operations and the college men with analysis (they were almost all males in those days, another anachronism compared to modern times). But there was considerable exchange and mutual learning because the ideal intelligence officer was supposed to be good at both analysis and operations in a crisis. Britain had a similar concentration of recruits from a very few, very prestigious schools like Oxford and Cambridge. Emblematic of the Achilles' heels of these old ways, the upper crust of social wealth and power dominated.

That presented growing problems when the Cold War generated proxy wars in Third World countries where English was a hated language, along with French or anything colonial, European or white, precisely the cultures and languages the children of wealth were fluent in. Of course there are still many places where expertise in banking is useful, and ability to blend into country club settings where the elites of Third World countries also gather. But more and more targets called for expertise in Arabic, Dari, Pashto, Farsi or African languages like Hausa (one of ~ 400 dialects in incredibly complex Nigeria, the largest country in Africa). Rich white men faced remarkable difficulty infiltrating terrorist cells or narcotics cartels, just by being tall, white, and standing out like a lighthouse in a storm no matter how good their language skills.

One of the more recent classic books that looked at collaboration between intelligence and university worlds was "Cloak and Gown" by Robin Winks[3]. And one of the more radical dissections of the weaknesses of this pattern of relationships between official spy agencies and a cloistered collection of upper-class colleges is Robert David Steele's "On Intelligence: Spies and Secrecy in an Open World"[4]. Steele was a decorated U.S. Marine Corps intelligence officer, then served 3 tours in operations for the CIA in Latin America. Then he went ballistic over the idiocies (and immorality) of bureaucracies and became an evangelist for Open Sources. His work in that domain was an important catalyst for creation of an "Open Sources" center at the CIA, which true to the traditions of *omerta* that still limit it today, classified its products after a couple of years of testing collaboration with academics unwashed by the clearance process. Understanding that challenge from both sides is a key to enlightenment here.

There were many other efforts to bridge this gap. The U.S. State Department had better success with many conferences that invited academics, partly because of the reality that the State department was less likely to kill or torture people overseas than the Pentagon or CIA. Some promising ventures like the Global Futures Partnership were begun by visionaries in the CIA like Carol Dumaine with other stars from allied agencies and NGOs. Israel's MOSSAD is infused by graduates of their best universities, the French DGSE by graduates of the Sorbonne universities, and Japan's finest are often led by graduates of Tokyo U. It is so around the world because intelligence agencies recognize sooner or later that actual intelligence is helpful, requires more than mere obedience to party lines, and that interdisciplinary education outside the boundaries of the security cleared world can help in many ways. Actual intelligence, and education outside of political or security boundaries, can in particular help detect falsehoods of great importance.

Politicization is a perennial problem in intelligence agencies, where analysis can be and often is skewed to please political bosses. Joshua Rovner explains the many dimensions of this common problem, but it is hard to grasp the scale of possible consequences[5]. For example, the invasion of Iraq by U.S. and allied forces on March 19, 2003 cost at least 2 **trillion** US dollars and the lives of at least 189,000 people (134,000 minimum estimated to be completely innocent civilians) searching for alleged weapons of mass destruction that did not exist[6]. In the words of Britain's Head of MI6 (Sir Richard Dearlove, found in the Downing Street memo,[7] **"The facts are (were) being fixed around the policy."** That is a very concise definition of politicization, and the estimated costs are certainly underestimates for many reasons.

In simpler words, intelligence "assessments" had been altered to justify an illegal and immoral war that had been desired by senior

American leaders long before 9/11 provided a false justification to invade a country that had not attacked us. Critical voices were silenced within the CIA, State Department's INR, and the Energy Department's intelligence unit. These were people who recognized that assessments were being distorted to serve a predetermined policy, silenced by prohibitions on telling our public the truths they needed to know. Thus a mortal sin occurred, a mortal sin with vast consequences, for us and for Iraq. My country, founded on concepts of freedom and duties to and of citizens, desecrated and wrecked its own Constitution.

Intelligence agencies are bureaucracies; ours became infatuated with secrecy, because of the universal recognition that sources and methods need protection AND the bureaucratic utility of hiding waste, fraud and embarrassments behind a broad secrecy shield. With that shield came institutional paranoia, fear of ethics and exclusion of contrary views, sometimes labeled "groupthink."That yields blindness to many things important to security and to other national objectives. Spy agencies still must deal with some of the world's most troubling problems, like weapons of mass destruction, terrorists and criminal banks. So it is not good to be estranged from the scholars. A kind of reciprocal hubris can occur, where the scholars scorn the spies as hopelessly immoral, and spies scorn the scholars on the grounds that they don't know essential secrets. This puts a strain on everyone that I discuss in a 2013 paper on ethics and WMDs[8].

Weapons of Mass Destruction have been with us for a while now and remain extremely important for obvious reasons. But current crises bring us global problems of unprecedented complexity. They may have military consequences but always have highly interdisciplinary causes, like transnational crime (and banking,[9]) clandestine arms trades, climate change, mass migrations and globalization of economies leading to persistent unemployment worldwide while elites are doing better than ever, as noted by George Maior, Director of Romania's SRI[10].

These newly important and very interdisciplinary problems put ever greater pressure on intelligence agencies to create productive liaison relationships with a much greater range of experts than times past, with deep knowledge of diverse kinds. During the Cold War, the nuclear physicists and engineers who developed nuclear weapons could be counted on to tolerate the significant restrictions of security systems, because their need was obvious with nuclear bombs, and the systems' enforcers were also their employers. But today, WMDs are just the beginning of a much longer list of things to worry about. One is retention. Half of the very bright recruits to the CIA leave within five years because they won't put up with the BS (otherwise known as the security rules). What is left are less than the best, but the agencies will never admit that. So now it is time to look in more detail at the Culture Chasm between pristine academies and messy but life-and-death important intelligence agencies today.

The Culture Chasm

I have alluded to several of the big differences between these tribes, the spies and the scholars, knowing that some real spies are brilliantly educated PhDs and such, and that some scholars make really good spies (well, a few do). There is overlap in both directions, and each group has many subtypes, but the skill sets are <u>not</u> identical. So to make progress I am going to pretend these are distinct tribes and itemize a few cultural characteristics that distinguish them. Lest this listing seem one-sided, please remember that I treasure both intelligence professionals and academics equally. They are both children of God, who under the right circumstances can serve country, humankind, and our Creator with distinction and honor. Or they can become Nazi doctors and thugs with fancy lapel pins, awards and degrees. The difference is all about what missions they choose to accomplish, which I <u>emphasize</u> is always **<u>their choice</u>** in the end.

Scholars tend to Value:	*while* ***Spies tend to Value:***
Open inquiry	Secret sources and assessments
“Truth” in a slightly unreal, abstract sense	The versions of truth that work best practically
Honesty	Effective deception
Clinical accuracy	Courage to face hard problems
Theoretical elegance	Practical utility
Years spent reading every comment	Good enough answers to hard questions FAST
Loyalty to abstract codes, creeds or law	Loyalty to the bureaucracy that hires them
Gentleness, and civic virtues	Ruthlessness, when faced with real enemies
Their reputation, which can be compromised by association with spies or spy agencies	Their secrets, which can be compromised by association with people who lack clearances
Peace	War, not intrinsically, but because professional intelligence systems are instruments of war, and were created to help states survive war threats.

As you may have inferred, most of these cultural differences stem fundamentally from the historic and modern fact that intelligence agencies are created by states to protect them from wars and war-like threats. Among military professionals, to take a different but related tribe, the need for secrecy of your operations and for good intelligence about adversaries is blindingly obvious. Recognition that death, killing, and deception are part of your work environment are also axiomatically obvious and true. That is a very different world than most academics live in, and much closer to a spy’s world. Thus military people tend to get along better with spies than many academics do, and they certainly are among the spies’ most consistent customers.

Now, the practical question for this paper is how best to maximize "Interdisciplinary, all-source" analytic results despite these large differences between the cultures of SMEs and classical spies. I will address the details of that in the next section soon, but want to embrace a concept called "strategic culture" first, one of the missions of Romania's Intelligence Academy. For best success at details it would help if the spies and the SMEs could share more of a common strategic culture. But what is that and how could it be made more common?

Alina Paun of SRI defines strategic culture "as the set of beliefs, attitudes and norms that impact on the assessment of threats and on the means deemed appropriate to make security"[11]. Even a good military alliance like NATO has problems achieving strategic harmony among its 28 members even though everyone is a classic nation-state with a hierarchical military structure. Military systems recognize better than most the power of unity of command, so they regularly convene groups to hammer out common strategic policies. Yet NATO still experiences big constraints, or let us say operational inefficiencies, due to differences among political entities that rule their 28 different democratically controlled military systems.

One of the keys to me is to focus on the truly fundamental and most universal security challenge, which is protecting the children and other innocents from the chaos of warring states. Every soldier understands that mission, and most academics do too even though they may be more inclined to talk or write when danger comes than to grab a gun. There is plenty of room in real-world operations for both diplomatic communications and kinetic options. If protecting the children seems passé, I say protect human civilization and your country from the forces of chaos that threaten us today, because the causes of war grow with every ignorant, unemployed male. And the ancient trick of sending the excess males off to kill each other in some foreign war does not work well in a world of Weapons of Mass Destruction with an Internet for organizing.

Ms. Paun reviews the great debates among political science theorists on this topic as good graduate students must, primarily from the European literature. If she had searched the Asian languages she would find similar syntheses[12,13]. I am more interested in practical solutions than theoretical, and more comfortable with incomplete analyses in time for use than allegedly perfect analysis too late to save our children or our civilization. So let us start now.

Partial Solutions

A porous security barrier

The absolute 'best people' simply will not agree to keep every secret no matter how evil. 99% of secrets are junk anyway; a few are critically important for the public to know because 'best people' seldom collaborate in war crimes. But all recognize the importance of keeping nuclear and other WMD recipes secret and operational military plans secret. Of course there are other issues; espionage is complicated. On the other side, if academics want to be trusted they need to be trustworthy and open to *accountability* if they reveal something that harms agents at risk, or otherwise wounds true national security. There is a middle ground between secrecy absolutism and libertarian extremes that professionals can recognize. Making it easier for prudent collaboration in that domain would help both groups.

A spirit of ecumenism

The ecumenical movement refers to theological efforts promoting respect for 'god's' wisdom as reflected in scriptures from around the world. The intelligence world needs a new, energetic spirit of ecumenism that embraces the religious thaw, but goes far beyond it. There should be more respect among academic disciplines, and more interdisciplinary work on great global problems like climate change. There should be more respect among the professions for the very difficult problems they specialize in, and there should be more respect between academics and spies. All are necessary to survive the rapids of dramatic change and occasional storms of violence ahead of our institutions, cities and children. Liaison relationships have been around for a long time – I am advocating ramping those up with a spirit of urgent ecumenism to meet the true threats of our unusually complicated times.

Better public diplomacy matched by less ruthless use of techniques from the dark side

Sure torture works *sometimes*, but poorly. It always has bad long term consequences in terms of prestige and real power. "Gentlemen" do not do torture, even when it is tempting, and they do not rationalize that, or illegal and immoral wars that may result. Such sins noted, polite society needs to know better and understand much better why good intelligence and even actual spies are **absolutely necessary** for group safety in our sometimes brutally violent world. So better public diplomacy by spy agencies would help a lot. That gets undercut when bullshit PR and advertising is passed off as diplomacy, as when agencies lie to the publics that pay their bills. Which is **often**. Then there is "targeted killing" – the latest term for one of the most ancient tools of tradecraft, assassination. Yes, murder can solve **some** problems, sometimes. But NO, the other costs are seldom worth the actual benefits over the long term. Disguising kidnapping and torture by euphemisms like "extraordinary rendition" does not fool anyone that matters.

Due respect for both long term and short term priorities, globally and for every tribe

One of the eternal tensions is between short term and long term; it has manifestations in every aspect of personal life and social interactions. The urgencies that spies attend to magnify this tension; because if you don't survive today's crisis the long term doesn't matter much, does it? Yet compromises made today so often bite tomorrow, and spies are wrong about as many things as everyone else in the end. So you do not want to bet the farm on every assessment. Similarly, a partial solution to the tensions between academic world SME's and classical spies is simply to respect their different cultures emphasizing the general need for speed in intelligence systems as opposed to the longer, less urgent and often broader views academics can bring to situations.

Cash for SMEs with less bureaucracy, and sympathy for spies despite their many flaws

Academics are accustomed to doing some things for free, at least not putting a cash register in front of every student.

Collaborations involving years of work are also common when research is being done on recognized merits from the base of institutions that provide support. But if governments want priority work from ‘best people’ they could better recognize the practical importance of paying them for long efforts. On the flip side, academics often think that spies are swimming in money with no clue how miserly their bureaucracies can be. Yes, bureaucracies can be rich pigs; that is true! Yes, there are beltway bandits in “intelligence” (commercial entities) that harvest billions every year in their bandity ways. But this does not mean the money flows down to individual agents easily. Tasks flow downhill naturally; money is less reliable. Finally, it could help to recognize what a royal pain in the anus and obstructer of operational efficiency bureaucracies can be for the truly effective, creative and hard-working spy[14].

Taming the greed and lust for power of bureaucracies, without illusions that academics will be better when given opportunities. Hubris and sloth are also indiscriminate vices

Here the last is most important. Hubris is extremely corrosive to wisdom which the bravest intelligence professionals should bring to their supreme commander or whatever policy person they are providing decision support for. The scattered universe of all data needs to be reduced in volume and greatly INCREASED in QUALITY when brought to the policy decider. Of course that quality increase begins with fact checking and similar elementary cleanings and filterings, but toward the end the best is infused with wisdom and other ephemeral qualities to bring out the best in what the “facts” are dealing with. One of the ancient pearls of IC wisdom says that analysts should not confuse themselves with the policy maker, <u>not</u> make policy, so they should stick to the facts necessary for the policy maker. True! But the best should still go beyond that if they can without violating the spirit of the bromide. All these aspects noted, have no illusions that academics are any more immune to hubris than spies (or to sloth, the root of greed). Many of our most urgent problems could be solved faster if the vested greeds and lusts were tamed. In shorter words, developing a professional ethos for spies and spy agencies could help a lot.

More collaborations among spies and academics like the Global Futures Partnership

"The Global Futures Partnership" is real, but a symbol here for the spirit of seeking effective collaboration across both national intelligence system boundaries, and disciplinary professional boundaries that separate operational spies from their less encumbered cousins outside the wire. Many academics would benefit greatly from your values added too. Large projects ultimately require funding to occur, and permission from many administrations <u>including</u> the security officers who cannot and will not disappear completely from intelligence organizations anytime soon. A recurring theme of this paper is suggesting that the security gremlins' power is too great today, and should be curbed. True; <u>Double</u> true. But gremlins remain necessary for the unexaggerated reasons they exist, the reality that spies from dangerous adversaries will still be trying to penetrate your organizations to do evil deeds for a long time. So counterintelligence is still necessary. That noted, let us try more collaborations with polite society even though they can be risky in their ways too. There is no risk free endeavor in the intelligence domain.

Focus on Corruption of Governance, at your peril; it is the most difficult threat of all. But Do ***<u>Focus</u>*** *on* ***it****, because reducing that is a key to survival of our civilization*

Corruption of governance is actually the most dangerous threat that most intelligence professionals will face in their careers. This is because the governments that fund spy agencies want them to steal other people's secrets, not their bosses. But if intelligence agencies do not reform the systems that empower them, who will? And if not now, when? The cost of delay is vast today.

The Interdisciplinary Future, and Transformation of the Global Intelligence Enterprise

"Best Practices" in our world of interdisciplinary problems metastasizing in novel ways today with technology morphing rapidly to create new words and realities like "Cyber Warfare" and "Bioweapons Expert" calls for radical transformation of the security clearance barriers, doctrines and cultures that I have commented on here and especially of the bureaucracies that underlie those barriers, doctrines and cultures. Changing cultures is much easier to say than do.

One of the greatest challenges will be developing a professional ethos for spies. Ethics for spies seems oxymoronic, yet it is a true key to survival in the third millennium and beyond.

Warriors everywhere should contemplate alternatives here, now and urgently. The developing global crisis is real, and threatens everything under heaven including each of our jurisdictions and loyalties. I will characterize that crisis more precisely for the cadets who are the future of Romanian Intelligence. To current professionals I say get with the revolution in intelligence and security affairs without leaving your institutions, so that when they are forced to change you will know how to advise them and help us all to survive. If we survive, our commitment to protecting the children, our countries and our civilization can be maintained.

References

[1] Gabriel, Sebe. "On the Evolution of OSINT: The Open Source Revolution and the Media," in *A Mind War: Intelligence, Secret Services* and *Strategic Knowledge in the 21st Century*, George Cristian Maior (ed.), (Bucharest, Editura RAO, 2010).

[2] Sun, Tzu. *The Art of War*. As translated by Samuel B. Griffith in the Oxford University Press edition of 1963.

[3] Robin, Winks. *Cloak and Gown: Scholars in the Secret War*, 1939-1961. (New York, NY: Morrow, 1987).

[4] Robert David, Steele. *On Intelligence: Spies and Secrecy in an Open World*. (Fairfax, VA: AFCEA International Press, 2000).

[5] Joshua, Rovner. *Fixing the Facts: National Security and the Politics of Intelligence*. (Ithaca, NY: Cornell University Press, 2011).

[6] Costs of War Project of the Watson Institute for International Studies at Brown University, in Providence, Rhode Island USA, 2013. The project is accessible at: http://costsofwar.org/Their report on the ten year anniversary of this war can be found at: http://costsofwar.org/iraq-10-years-after-invasion.

[7] Sir Richard, Dearlove, head of MI6 (Britain's foreign intelligence agency). The quote comes from a "Downing Street Memo" that is actually minutes of a meeting transcribed during a gathering of many of the British Prime Minister's senior ministers on July 23, 2002. Published by The Sunday Times on May 1, 2005, this document was the first hard evidence from within the UK that exposed the truth about how the Iraq war began.

[8] Michael, Andregg. "Ethics of Nuclear Weapons and National Security Intelligence," prepared for presentation at the ISA international ethics section on April 6, 2013. Not published but available from mmandregg@stthomas.edu.

It includes more details on how false evidence used to sell the invasion of Iraq was altered or even manufactured.

[9] Susan, Blair. Interview on “Moyers and Company”, Public Broadcasting System, USA. “What Big Banks are Getting Away With” on Friday, 22, March 2013. Accessible at: http://billmoyers.com/

[10] George Cristian, Maior, and Sergei Konoplyov, (eds.), *Strategic Knowledge in the Wider Black Sea Area*. (Bucharest, Romania: Editura RAO, 2011).

[11] Alina Sinziana, Paun. “NATO’s Strategic Culture: Drivers, Characteristics and Future Evolution.” This is her unpublished Master’s Thesis for an MAS in International and European Security from the Geneva Centre for Security Policy, University of Geneva, Switzerland, 29 April, 2011.

[12] Sato Tokutaro and Hara Shobo. “Strategy of Ocean States and Continent States,” 1973.7.15, pp. 282-283.

[13] Inazo Nitobe. *Bushido: the Soul of Japan*, (Kodansha International Ltd., First Edition, 2002).

[14] Ishamael, Jones (alias). *The Human Factor: Inside the CIA’s Dysfunctional Intelligence Culture*, (New York, NY: Encounter Books, 2008). “Jones” was an astonishingly productive case officer for a long career with CIA. Like many others like Robert David Steele, he left disgusted by the inefficiencies and ultimate immorality of the intelligence bureaucracies that he knew quite well.

‘Actionable’ Intelligence Is Not ‘Warning’ Intelligence

Jan GOLDMAN[*]

Abstract

There has always been pressure on the U.S. intelligence community by both the public and policymakers to forewarn impending threats. Intelligence, when performed correctly, is the use of information to foresee events, actions or possible decisions by an adversary. The term most commonly used is actionable intelligence. It is a term that has been heralded by the policymaker and unfortunately embraced by the intelligence community. It is a term that is a seemingly a ‘win-win’ for everyone. It is a term that allows people to understand and appreciate the significance of intelligence. Actionable intelligence is defined by the policymaker not by the intelligence community. The result has been extremely confusing for both intelligence analysts and policymakers. The epistemology of forecasting for intelligence analysis, that is to know the difference between intelligence failures and warning failure, can possibly be the focus on how knowledge is managed to the recipient of that product produced rather than the intelligence collected. This is called knowledge management. The two types are descriptive analyses and inferential analyses. Without a doubt, ‘intelligence failure’ and ‘warning failure’ are considered equal parts of a forecasting equation when there is a failure to understand these concepts as separate entries. Consequently, this has allowed such a term as ‘actionable intelligence’ to exist. In the end, it is only after ‘intelligence failure and ‘warning failure can be clearly understood and defined that we can improve forecasting and intelligence that we can bypass this poorly defined term, “actionable intelligence” in warning intelligence.

Keywords: actionable, epistemology, forecasting, intelligence failure, warning

The worldwide intelligence community (WIC) should have its own lexicon, similar to any other evolving profession. Lawyers and doctors have their own terminology which is found in legal and medical dictionaries, respectively, regardless of country. Although the worldwide intelligence community has no specific source for definitions, it is not surprising intelligence professionals and the public understand commonly understood words such as “espionage”, “disinformation”, or “source validation.” However, even a foundational term used in the Intelligence Community such as “intelligence cycle” may require an explanation. This is because each

[*] Professor, Georgetown University, USA

agency in each of their nation's intelligence community may have its own definition. For example, in intelligence analysis training one agency includes a five-step intelligence cycle, while another agency teaches a six-step intelligence cycle. Both agencies are in the same intelligence community serving the same nation. The intelligence profession is evolving, and along with this process comes a maturity of language based on a common process.

However, there is a word that is continually used with little understanding of the definition of that word. It is a word that seems to have no definition, and is solely dependent on the speaker, rather than the process. The term is "actionable intelligence." The term "actionable intelligence" has no meaningful understanding within and outside the USIC, which has allowed this term to be misused resulting in confusion by policymakers, intelligence personnel and the American public.

There has always been pressure on the U.S. intelligence community by both the public and policymakers to forewarn impending threats. Intelligence, when performed correctly, is the use of information to foresee events, actions or possible decisions by an adversary. While intelligence can be used as evidence (i.e., to prove an event, action or decision has occurred). Intelligence when received within a timely manner can be used to anticipate the future. Intelligence can be used as evidence at a trial and evidence can be used as intelligence. Of course, evidence of a possible threat is called "indications" of a future scenario. This should not be confused with developing the scenario, which is based on indicators.[1] It can all be very confusing.

During Gulf War in 2003, British troops in Iraq were seeking evidence of America's claim that Iran was providing weapons to Iraqi militias, one British officer said, "I have not seen any evidence – and I don't think any evidence exists – of government-supported or instigated' armed support on Iran's part in Iraq...It's a question of intelligence versus evidence...one hears word of mouth, but one has to see it with one's own eyes. These are serious consequences, aren't they?"[2]

What separates intelligence from evidence is that the former is mostly used to anticipate the future, while the latter is used to explain the past. This is one of the basic tenets of the expectations of *any* item (e.g., National Intelligence Estimate) for consumption produced by the national intelligence community. A nation relies on its intelligence community to collect and process information with the result of having a product that allows commanders or policymakers, to make the right decision. The intelligence community seeks to produce assessments based on either qualitative or quantitative analysis of an impending threat.

This was reiterated in 2006, when U.S. Intelligence Community Directive #201, re-established the National Foreign Intelligence Warning System (NFIWS). According to the document, the goal of the NFIWS is to provide warning in enough time, and with sufficient information, to allow our leaders to proactively confront emerging challenges, leverage opportunities, avoid surprise, and produce strategic outcomes favorable to the United States. Although most of this document is redacted in the public domain, just above the Director of National Intelligence John Negroponte's signature are these statements,

The NIO/W (National Intelligence Officer for Warning) is hereby designated the DNI's primary executive agent for foreign intelligence warning and assigned the authority to direct, manage, and certify the capabilities, processes, and performance of the NFIWS......Warning is a priority mission for all IC [Intelligence Community" elements and their personnel."[3]

If one knows the capability and intention of their adversary, they are that much smarter in predicating, or rather forecasting the threat. However, a failure to provide and execute such a useful product from the intelligence community is likely to leave the commander or policymaker without capable intelligence. In other words, there is an "intelligence failure" to support the decision-maker. In the past, "intelligence failure" has been narrowly relegated to a breakdown to collect or analyze information correctly *and* in a timely manner.[4] Unfortunately, a new term has entered the lexicon between the decision-maker and the intelligence community. It is a new term that avoids the stigma of the policy and intelligence communities to tolerate "intelligence failure." It is a term that seeks to make intelligence "doable" because it seeks to cause some type of action or response by the consumer. It is intelligence that requires *immediate* action.

The term most commonly used is *actionable intelligence*. It is a term that has been heralded by the policymaker and unfortunately embraced by the intelligence community. It is a term that is a seemingly a 'win-win' for everyone. It is a term that allows people to understand and appreciate the significance of intelligence. If knowledge is power, then *actionable intelligence* is supreme authority over your adversary in a timely manner to reduce immediately and effectively all harm. A quick review of the U.S. Intelligence Community reveals only one possible legitimate definition of "actionable intelligence." At the Department of Justice, an "actionable lead" is information that could later be turned into a prosecution of individuals. However, an "actionable lead" is dissimilar from "actionable intelligence." According to the previously established National Drug Intelligence Center (NDIC), actionable leads were used for exploiting information for possible arrests (i.e., tactical intelligence) as well as reports to policymakers at the strategic level (which is referred to as actionable intelligence). According to NDIC's 2010 fiscal year strategy it, ...supports policymakers by providing timely strategic intelligence on the production, consumption, and trafficking of illegal drugs. This is done through information collection and analysis from law enforcement and national security agencies. NDIC also maintains operations to exploit seized documents and computer equipment for drug related intelligence and **actionable leads**. Along with producing timely and **actionable intelligence** NDIC annually produces the National Drug Threat Assessments well as regional and collaborative international drug threat assessments.[5]

Unfortunately, for the remainder of the U.S. Intelligence Community, the term, "actionable intelligence" is a myth, yet, it continues to be something chased by both consumers and intelligence practitioners. It provides false hope to the public and it raises unrealistic expectations. It can be a destructive allegorical term that glosses over the boundaries of intelligence failures and warning failures. This does not mean intelligence cannot be 'actionable'; rather, it is a contention of this article that no specific and separate category of intelligence in national security should be labeled "actionable intelligence." On the contrary, the term "actionable intelligence" undermines the usefulness of all intelligence. Consequently, until the intelligence community highlights the false promise and unrealistic expectations of actionable intelligence, the intelligence community may likely be at a disadvantage in its perception of competency with policymakers and the public, making it easier for the media to indict the intelligence community with the question, "Why didn't you tell us?"

Defining "Actionable Intelligence"

In 2014, at least three books were published on "actionable intelligence" and none of the books focus on national security. The three books that mention this term focus on business or personal and professional development.[6] In 2013, thirty books on business, desktop and web applications, digital media, and engineering included chapters on "actionable intelligence."[7] In Washington, D.C. a three day "Actionable Intelligence Summit"[8] was held on such "key topics" as, "Evolving efforts to improve national security and international stability through IAP [not defined]; Transforming strategies supporting international intelligence community cooperation and interoperability; Best practices for interagency cooperation between DoD, DHS, DoS, DoJ, and the military services; Requirements and modifications that support more efficient, adaptable intelligence analysis." Other topics included "Intelligence, Integrity and Information Sharing" and "The Counterintelligence Threat from Non-State Actors." These may all be worthy topics, but they fail to highlight the "actionable" aspect of intelligence.

Recently on a national security blog, it was asked if there was a good definition of "actionable intelligence." Several people responded and wrote their interpretation of "actionable intelligence." Unfortunately, having a standard interpretation for "actionable intelligence" is not the same has having a standard and accepted definition by an established community. Conversely, if you seek an official definition of "intelligence" at least a dozen different definitions exist within and outside of the U.S. intelligence community. Generic definitions for "intelligence" that are typically found in federal agency lexicons, include "secret information, especially about an actual or potential enemy or an agency, staff, or office employed in gathering such information"[9] or the more specific, "the product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to domestic and foreign activities and to domestic and foreign or US and enemy-held areas."[10] According to the CIA, intelligence is "reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us. Intelligence is the prelude to decision and action by U.S. policymakers. Intelligence organizations provide this information in a fashion that helps consumers, either civilian leaders or military commanders, to consider alternative options and outcomes. The intelligence process involves the painstaking and generally tedious collection of facts, their analysis, quick and clear evaluations, production of intelligence assessments, and their timely dissemination to consumers. Above all, the analytical process must be rigorous, timely, and relevant to policy needs and concerns.[11] Nevertheless, although every organization has its own definition of "intelligence, Michael Warner wrote in the Studies of Intelligence Studies, "Wanted: A Definition of "Intelligence'", that we need to separate the reality from the perception of this word. He further discusses the role of information in the intelligence process.

But actionable intelligence has clearly a perception of action. And as singular a definition we perceive it to have, but, yet, there is still no "official" definition of this word by any nation's intelligence community. This resulted in deadly consequences for the United States, when President Bush said that an intelligence memo he read shortly before September 11, 2001 contained no actionable intelligence that would have helped him to try to prevent the 9/11 attacks. The memo appeared on August 6, 2001 entitled, "Bin Laden Determined to Strike in US." According to press reports, Bush said, "What I wanted to know as is there anything specifically going to take place in America that we needed to react to."[12] In another example, National Security Advisor Condoleezza Rice said it would not have mattered to have senior officials form the intelligence and law enforcement communities to meet regularly in the summer of 2001 to sift through the warnings that preceded the 9/11 attacks. Rice believed that there were not enough specifics or "actionable intelligence" to justify such meetings. Nevertheless, lower-level officials, led by National Terrorism Chief Richard Clark, met regularly. According to Clark, "when you're told there's going to be a major terrorist attack, but ho, by the way, we don't know where or when, that's all the more reason to put down whatever else it is you're doing...roll up your sleeves and get involved in trying to find that 'actionable intelligence'.[13]

Actionable intelligence is defined by the policymaker not by the intelligence community. Actionable intelligence has no objective meaning. Policymakers determine what it is or is not actionable. In reality, it is a notional concept (something that does not exist); it requires no analysis or assessment....similar to yes or no warning. It leaves little to gray area. A quick search to define the term is one that deals with no time...computers. According to one cyber encyclopedia, actionable intelligence is "Having the necessary information immediately available in order to deal with the situation at hand. With regard to call centers, it refers to agents having customer history and related product data available on screen before the call is taken."[14]

Currently there is no official definition of actionable intelligence in the United States Intelligence Community. In an official document focusing on the future threats to the United States (ODNI Memorandum #2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide,*) there is no mention of "actionable intelligence". Instead, this memorandum which seeks to foster cooperation among and within the community focuses on "...the IC [intelligence community] meet its obligation to provide and make available timely warning, analytic insight, and intelligence information to all customers and other intelligence components as needed to meet national security objectives, while protecting intelligence information and intelligence sources and methods."[15]

Although there is no agreed definition for "actionable intelligence", it has come to be a shorthand term for responding to intelligence, at the tactical level in the absence of policy. The result has been extremely confusing for both intelligence analysts and policymakers. For example, in the summer of 2001, prior to the terrorist attacks of September 11, National Security Adviser Condoleezza Rice said there were not enough specifics or "actionable intelligence" to justify any meetings between senior intelligence officials and members of the National Security Council. Additionally, President Bush said the intelligence memo he read shortly before the 9/11 attacks contained no "actionable intelligence" that would have assisted him in preventing the terrorist's actions. However, what is the opposite of actionable intelligence? Would it be "un-actionable intelligence?" When does intelligence become useful? Or is the value and usefulness only something the policymaker or intelligence analyst adds to the information?

The epistemology of forecasting for intelligence analysis, that is to know the difference between intelligence failures and warning failure, can possibly be the focus on how knowledge is managed to the recipient of that product produced rather than the intelligence collected. This is called knowledge management. Knowledge management develops a functional taxonomy based on the type of analysis and the temporal distinction of knowledge and foreknowledge – warning, prediction, and forecast – which distinguishes the primary categories of analysis.[16]

These two types are descriptive analyses and inferential analyses. To understand descriptive analyses it is important to know that it provides little or no evaluation or interpretation of collected data. This leaves the person reading the report to develop subsequent interpretations. Typical descriptive analytics tasks include organizing, compiling, structuring, indexing and cross-checking. Any of the intelligence collection platforms (e.g., signals intelligence, human intelligence, imagery, etc...) can produce descriptive analysis. Unfortunately, when the information collected under descriptive analysis, requiring little or no evaluation or interpretation, transcending intelligence material, it may incorrectly be put into the context of warning intelligence. The result is that the reader may be forced to do something, or what has been commonly referred to as “actionable intelligence.”

The term “actionable intelligence” seeks to remove any ambiguity that may be prevalent in the original intelligence message. In reality, this almost notional intelligence is a rarity in any intelligence organization. For example, when the United States had intercepted Japanese message traffic prior to the attack on Pearl Harbor, not one of the messages was deemed convincing enough because there was no reporting of the stated day, time, or avenues of approach of the attack. In other words, policy makers were looking unrealistically for intelligence to clearly state the time and location of the impending attack, In part, this is because consumers of intelligence want a theoretical system that provides a clear understanding for intelligence services, to tell them that there will either be an attack or not, so that appropriate counter-mobilization actions can be taken, or not.

While a warning system that policymakers can rely upon so that uncertainty is removed from the decision-making process is attractive, unfortunately it is not a realistic objective, the theoretical problem with this system is that while there will inevitably be indication of the other sides’ intentions to do harm, especially in hindsight, these can easily be lost in the noise of contrary or ambiguous indications. Mostly successful surprise attacks occur ‘not out of the blue, but out of a murky grey which did not fit well into the Yes/No warning model.[17]

An inferential analysis requires the intelligence analysis of collected relevant data sets (this is known as “evidence”) to infer and synthesize explanations that describe the meaning of the underlying data, Using inferential analysis to view the past, present and anticipate the future is to explain past events by describing structure attributes and behaviors, in relation to predicting future events.

Accordingly, all intelligence analysis can be divided by two types of knowledge, that which is either explicit knowledge or tacit knowledge. When we use explicit knowledge, it is to capture and codify thoughts in abstract human symbols... It is the basis for logical reason and most importantly of all; it enables knowledge to be communicated electronically and reasoning process to be automated. Data can be stored, retrieved and analyzed. For producing warning intelligence, this is considered the better form of knowledge. On the other hand, tacit knowledge is the intangible, internal, experiential and intuitive knowledge that is undocumented and maintained in the human mind. It is a personal knowledge contained in human experience. This kind of knowledge forms the bridge between perception and the high forms of conscious reasons that can be described more easily. According to Waltz, "This is the personal knowledge that is learned by experience, hones as a skill and often applied subconsciously."[18]Tacit knowledge adds value to the process, and allows an analyst to assess any preventive action by an adversary. These two forms of knowledge, as well as two modes of human thought, have been described as 'know-what' (i.e., explicit knowledge) and as 'know-how' (e.g., tacit knowledge), distinguishing the ability of *tacit* knowledge to put *explicit* knowledge into practice.

Without a doubt, 'intelligence failure' and 'warning failure' are considered equal parts of a forecasting equation when there is a failure to understand these concepts as separate entries. Consequently, this has allowed such a term as 'actionable intelligence' to exist. These is a term that means, 'do something' which in reality, may not require any analysis but rather an observation or perceptions of some action. For this, one can easily watch current intelligence (that which appears on live television) to determine a response. The epistemology of intelligence seems to provide a breakdown of the components of knowledge of intelligence into distinct categories. Using such theories can assist in better intelligence collection, as well as in utilizing this knowledge in forecasting in international affairs. Through this essay, the reader has been introduced into both the vocabulary and theory of ideas that have the ability to further develop and delineate 'warning' form the general concept of information as 'intelligence'. In the end, it is only after 'intelligence failure and 'warning failure care clearly understood and defined that we can improve forecasting and intelligence that we can bypass this poorly defined term, "actionable intelligence" in warning intelligence.

References

[1] An "indicator" is a future act, event or decision; however, once the act, event or decision occurs it becomes an "indication."

[2] Ellen Knickmeyer,"British Find No Evidence of Arms Traffic From Iran" by, *Washington Post*, October 4, 2006.

[3] United States Government, "Intelligence Community Directive, Number 201", Federation of American Scientists, accessed 6 July 2014 at http://www.fas.org/irp//dni/icd/icd-201.pdf

[4] "Timely manner" should be defined as the ability to react with enough time to react with total effectiveness.

[5] The National Drug Intelligence Center closed on June 15, 2012, after beginning operation in 1993. See, Department of Justice website, http://www.justice.gov/jmd/2010summary/pdf/ndic-bud-summary.pdf

[6] The three books include *Find Out Anything From Anyone, Anytime* by James Pyle and Karinch Maryann (Career Press, 2014), *Ask, Measure, Learn* by Lutz Finger and SoumitraDutta (O'Reilly Media, 2014) , *Definitive Guides for Supply Chain Management Professionals* by Robert Frankel and others (Pearson, 2014).

[7] A search of Safari Books On-line, ProQuest, and the terms "actionable intelligence" provided no results.

[8] The Actionable Intelligence Summit was held August 26-28, 2013 at the Washington Plaza, in Washington, DC, http://www.actionableintelsummit.com/MediaPartner.aspx

[9] *The American Heritage® Dictionary of the English Language*, Fourth Edition copyright ©2000 by Houghton Mifflin Company.Updated in 2009.Published by Houghton Mifflin Company.

[10] Leo D. Carl, *International Dictionary of Intelligence* (McLean, VA: Maven Books, 1990).

[11] CIA, Washington, DC, September 1993, updated Feb. 1994.

[12] CNN, "Bush: Memo had no 'actionable intelligence' accessed on 7 July 2014, http://www.cnn.com/2004/ALLPOLITICS/04/11/911.investigation/

[13]"Rice Testifies at Hearing" *USA Today*, 8 April 2004, page 1.

[14] PCMAG.com, "Encyclopedia" accessed 1 July 2014 at http://www.pcmag.com/encyclopedia_term/0,2542,t=actionable+intelligence&i=37443,00.asp

[15] Office of the Director of National Intelligence, Intelligence Community Policy Memorandum Number 2007-200-2,ODNI website, accessed on 1 July 2014 at http://www.dni.gov/electronic_reading_room/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf

[16] Edward Waltz, *Knowledge Management* (Norwood, MA: Artech 2003), p. 11.

[17] Robert Brody, "The Limits of Warning," The Washington Quarterly, vol. 6, no. 3, 1983, p. 40-48.

[18] Eduard, Waltz, *op. cit.*, p. 64.

Neither Overt Nor Covert: New Sources For Intelligence in the XXIst Century ?

Eric MECHOULAN[*]

Abstract

In 1948, George Orwell imagined a world where all of us were under the permanent scrutiny of Big Brother. 55 years later, we are witnessing a collective mad rush to put one's private life on display. 65 years later, our objects will do it for us. Tomorrow, everything we use will leave traces for us, and about us. I would like to share with you a few ideas about these "things", all the objects (clothes, consumer goods in general; medical sensors, energy management tools...) that will be connected to the Internet of things, that has been anticipated since the end of the 20th Century.

Here are some questions to raise very briefly.

What will be the new sources for tomorrow's Intelligence and to what extent will they call for a complete renewal of OSINT?

What will be the consequences on the Intelligence Services and their political framework?

Keywords: OSINT, new sources, data, intelligence

Our things... without us as sources for Intelligence

The near future is a world in which most objects will be equipped with identifiers that do not depend on us any more, unlike today's computers. The Internet of things will transform this world of human responsibility for most of data capture. Objects, from transcontinental planes to refrigerators, will have their own identifiers and will develop interfaces and modalities to connect and interact with users and of course other objects without our request or knowledge (M2M, for Machine to Machine). They will exchange data about everything, that will be stored... somewhere. So shall we, when the human body is activities get interconnected themselves and our "quantified self" becomes part and parcel of the network.

Thus, Intelligence opportunities seem as infinite as possibilities to escape this world are minimal. This evolution demands that Intelligence Services be also ready to face new challenges: those of quantity, quality, and access.

Quantity means either data, metadata or big data. Intelligence Services are accustomed to this issue. However, the amount of data that will be produced in a world of interconnected material and immaterial objects is hard to conceive. From big data, we shall pass to very big data, the processing of which will allow Services to spot patterns and potentialities. Traces become the basis for a new

[*] Intelligence expert, France

predictive analysis when coupled with prediction markets and collective Intelligence solutions, turning each of us into an unwilling source informing someone, somewhere, of our next actions.

In terms of quality, things will behave the way humans will prepare them to influence and manipulate, lie and deceive, in other words erase their traces or create misleading ones, the same way people already live imaginary lives on social networks. To put it in a nutshell, whatever communicates is a potential spy, hence a potential source or ally for Intelligence people, but also a target for their enemies.

Monitoring and understanding our adversaries' capabilities to perform a similar absorption and interpretation of data will also be part of the Intelligence business. In that game, Services will carry little weight compared to private business and their problem will be that their leverage on private business might be reduced far more that they can expect or anticipate.

Will these traces be private or public? They might remain for some time in an in-between situation that cannot become an ideal space of action for Intelligence gatherers. For some time because, as King Midas turned into gold whatever he touched, the law turns into law whatever it touches. And the law runs fast, especially in societies abiding by the rule of Law. Access to this mass of information from private companies or from countries that will enshrine their data will become an Intelligence challenge, legally and materially.

Besides, most if not all traces will be encrypted, made "anonymizable" or "self-destructible", whether we want it or not, by their designers, both to avoid hacking and to sell better by gaining public confidence. For confidence will become more and more the core of the system and, unfortunately, breach of confidence actions do not come from those we expected, i.e. the hackers, but by State players. The fear of being spied on by Intelligence Services a fear that leads more and more users to encrypt their communications must be regarded as a trend that might lead every single "thing user" to become the protector or the guard of the most dangerous people on earth, whether terrorists or criminals.

Some information that is public might become private with time, contrary to the 20th Century trend which, when private information could be released into the public domain after a certain number or years. And, in this not so far future, we might be talking of seconds. Then, the challenge will be to spot them in time and the issue of the data retention period will change dramatically.

The legality of many forms of intrusion will evolve faster than expected by Intelligence Services and accessing overt information might, at some point, require covert operations.

Consequences on Services

Intelligence Services, as well as armies, regard themselves as the ultimate protector of the State, the only legitimate representative of the nation, and the last barrier defending its sovereignty.

What is our State? To put it simply, it is the structure that men first built collectively in order to put an end to the struggle of everyone against everyone in the quest for a limited quantity of riches; then, by contract with the State, citizens agreed to abide by its rules, rules that they eventually elaborate together in a democracy. Beyond this basic *raison d'être*, the State, particularly in Europe, extended its functions to the production and management of public services and even goods, the creation of a Welfare State and the safeguarding of ever-increasing rights.

The problem is that, at the collective level, the emergence of the interconnected world of the 21st Century goes together with a rising diffidence towards an impoverished and untrustworthy Western State that spies on citizens in order to perpetuate itself at their expense, far from being the best guarantor of their rights. As for the production and management of goods and services, the rationalized economy promised by the Internet of things is supposed to render the State anachronistic and irrelevant. The psychological evolution induced by technology, the evolution of privacy, identity, extimacy and thus secrecy will take place in a world where the State, sovereignty and their champions, including services, will not be the same.

In a world where objects communicate, where the economy wants to become increasingly self-regulated, distribution of power will evolve quickly and a strong temptation of extending some kind of automaticity to the organization of power and a distancing posture vis-à-vis the political sphere will emerge.

As for sovereignty, it will mean less and less to illiterate masses. Democracy will change also, probably not for the better. People will feel less and less need for intermediaries i.e. representatives. In an interconnected world where the feeling of privacy will be enhanced and that of public good will be reduced, people will tend to trust more their service providers – including security companies –, their groups, their tribes, than an anonymous and dangerous State. The survival of democratic societies might be in danger if the risk not staved off early enough.

Hence a double paradox for Intelligence Services. First, they will need more and more means to perform a modern State function that will probably be less and less required by people in a postmodern world. Second, they will need very different people to give a meaning to this amount of data, which will demand a culture and an understanding of societies that most Services lack already.

Then, Intelligence Services will have to think about what to do with this amount of very big data... but without thinking at the same time about their part in the regulation process and about the future of the institution that legitimates their action, i.e. the State, this major undertaking might be entirely irrelevant.

These are some of the challenges ahead of Intelligence Services in a world of traces.

* * *

These few remarks just scratch the surface of the topic.

Traces regulation concerning their nature, their access, their encryption, their storage period... will be more and more necessary and Intelligence Services have to anticipate and prepare the part they want to play in this regulation and guarantee its transparency. Because this part will be part of a wider challenge: the survival of the State.

As often in psychology and technology, practice will be ahead of theory, and it will take time before analysts understand the world soon to come. The challenge for Intelligence Services is not data overload. It is the adaptation of the Intelligence officer's brain. What is to be feared is the more data, the stronger the belief that all answers are inside, the less meaning and the less understanding. Too many Intelligence people mistook secrets for Intelligence in the 20th Century; likewise, too many will mistake data for Intelligence in the 21st Century.

Will secrecy be even more pricey? This is hard to assess. But one thing is sure: the French use to say "*Pour vivre heureux, vivons cachés*". This, never more.

Analists’ Perceptions Regarding Variables Influencing Intelligence Analysis

Cristian Anghel CIUPERCĂ[*]
Ella Magdalena CIUPERCĂ[*]

Abstract

Worldwide, there are only a few studies based on the results of certain scientific researches that investigate, sequential or not, the general aspects of intelligence analysis. The main explanation is that such a subject is difficult to approach due to the nature of this type of work and, also, because any research efforts would be hardly widespread as the world of intelligence continues to look like a caste whose rules, techniques, tools and methods remain inaccessible to the public. However, unlike the methods and results of data collection (which remains a secret field), the way analysts evaluate information starts to be a transparent process, and this could have positive effects in terms of consolidating an efficient security culture. Therefore we conducted a questionnaire based-research in order to review the main variables that affect the work of Romanian intelligence analysts.

Keywords: intelligence, analyses, survey, questionnaires, biases

Introduction

Worldwide, there are only a few studies based on the results of certain scientific researches that investigate, sequential or not, the general aspects of intelligence analysis. The main explanation is that such a subject is difficult to approach due to the nature of this type of work and, also, because any research efforts would be hardly widespread as the world of intelligence continues to look like a caste whose rules, techniques, tools and methods remain inaccessible to the public.

However, unlike the methods and results of data collection (which remains a secret field), the way analysts evaluate information starts to be a transparent process, and this could have positive effects in terms of consolidating an efficient security culture. Prestigious universities opened their gates for masters where intelligence experts teach within the field of open source intelligence analysis. Also there are private firms carrying out synthesis and forecasts for government agencies.

[*] PhD, “Mihai Viteazul” National Intelligence Academy, Romania

[*] PhD, “Mihai Viteazul” National Intelligence Academy, Romania

There are quite a few types of training and specialization of analysts in Romania although lately analysts' role in intelligence work has greatly increased. For the Romanian Intelligence Service analysis and forecasting activity is considered to be "...an essential component of an intelligence service activity... provides analysis for decision makers, consumers of information on which they make decisions, decisions that affect all of us in a highly interdependent world, situated under a fantastic pressure, having positive and negative connotations as a result of globalization" (Maior, 2008).

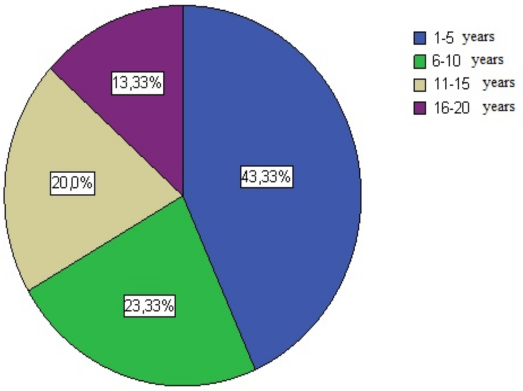
But not all analytical products are complete and not all forecasts are accurate. Although analysts strive to reduce the number of errors, some analyses still contains some. Intelligence failures are not generated by the lack of data, but especially by the faulty manner in interpretation of the way they can correlate and reveal their meaning (Davies, 2009). So the main problem of nowadays analyses seems to be the ability to decode and interpret the available data.

Psychologists have identified a number of subjective reasons (availability bias, illusion of causality, the lack of a mental model), but it is still questionable if they are the real key problems as there are also a lot of external factors such as time pressure, insufficient data that might influence the analyses. Which type of variables are stronger and what is the way to minimize them? This paper presents the results of a sociological survey conducted in order to identify the problems analysts have to face and factors that are generating, in their opinion, errors in intelligence analysis.

The methodology of research

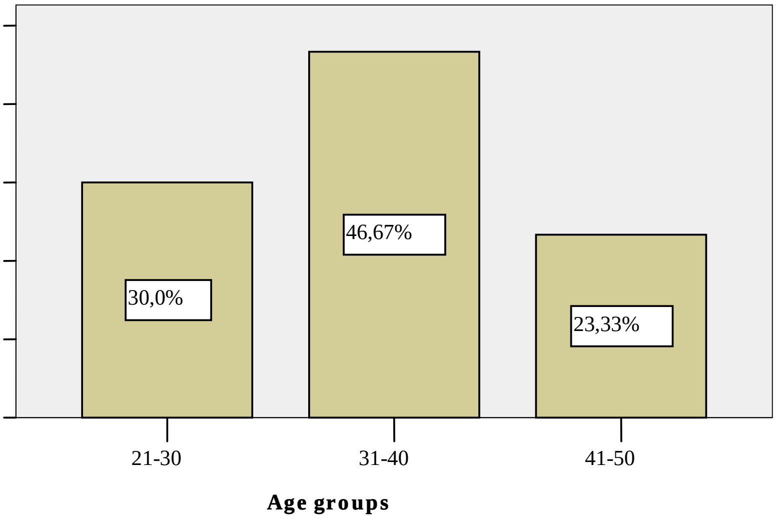
To reach the objective of the research we applied a questionnaire to a sample consisting of 30 analysts of Romanian Intelligence Service, 20 of them female and 10 male. Their experience of work in their domain is represented in Figure 1.

Figure 1. The assignment of intelligence analysts by their working experience



Also, the distribution according to age ranges, representative for the age distribution of all analysts, is presented in Figure 2.

Figure 2 – Assignment of analysts group by age



Results and discussions

Most of the investigated analysts proved a good self-image and revealed a high self-esteem, as 80% of them describe themselves in positive terms (see Chart 3).

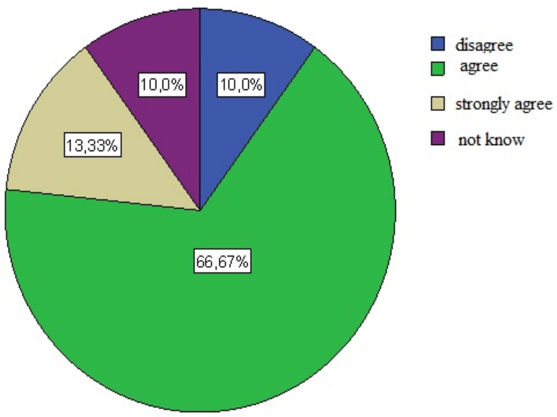


Figure 3: Do you consider yourself a good analyst?

However, only 20% of subjects, who considered themselves to be good or very good analysts, maintain their views on the analysis long after they have delivered it. The rest of them change their opinion to a greater or lesser degree. Also, top analysts deliver more often analytical products without sufficient information comparing with those whose self-perception is slightly diminished. This may be an effect of confidence in their own skills but in this context one should remember that over evaluation can generate negative consequences. Moreover top analysts do not evaluate low memory, the pressure of time or routine as key factors in the occurrence of errors in the analysis, while the common ones share this idea.

Regardless of how they perceive themselves, over 30% of respondents consider they have knowledge gaps in the fields where they are specialized for doing analytical products. Therefore half of them need the advice of someone else (see Table 1).

Table 1 – Self-perception of expertise (percents)

Doing an analyses to what extent did you feel like:	Strongly agree	Agree	Disagree	Strongly disagree
Having knowledge gaps in that field?	-	33,3	56,7	10
Needing an advice from someone else?	6,7	43,3	46,7	3,3

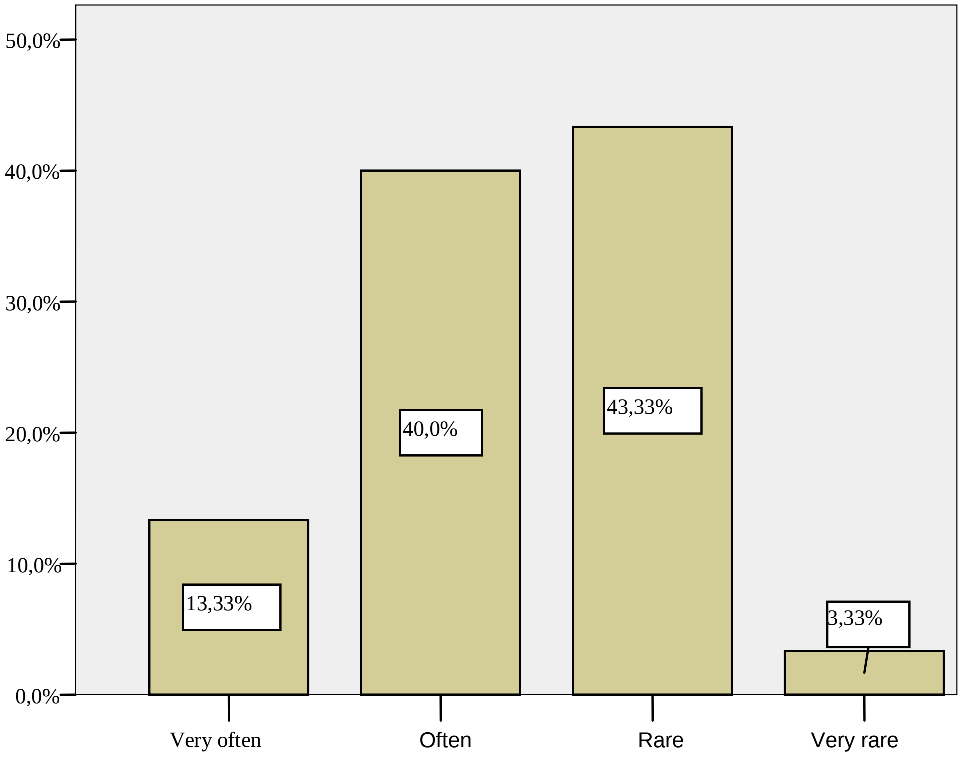
Regarding the variables that would cause errors in intelligence analysis, the biggest influence is associated with insufficient data and information, low level of intelligence, irrelevance of the expertise in the field and the existence of prejudices (see Table 2).

Table 2 – Variables generating errors (in percent)

Do you agree these variables are generating errors?	Strongly agree	Agree	Disagree	Strongly disagree	Not know
Lack of information and data	53,4	43,3	3,3	-	-
Low level of intelligence	63,4	33,3	-	-	3,3
Irrelevance of the expertise in that field	43,3	50	6,7	-	-
Prejudices	36,6	50	6,7	6,7	-

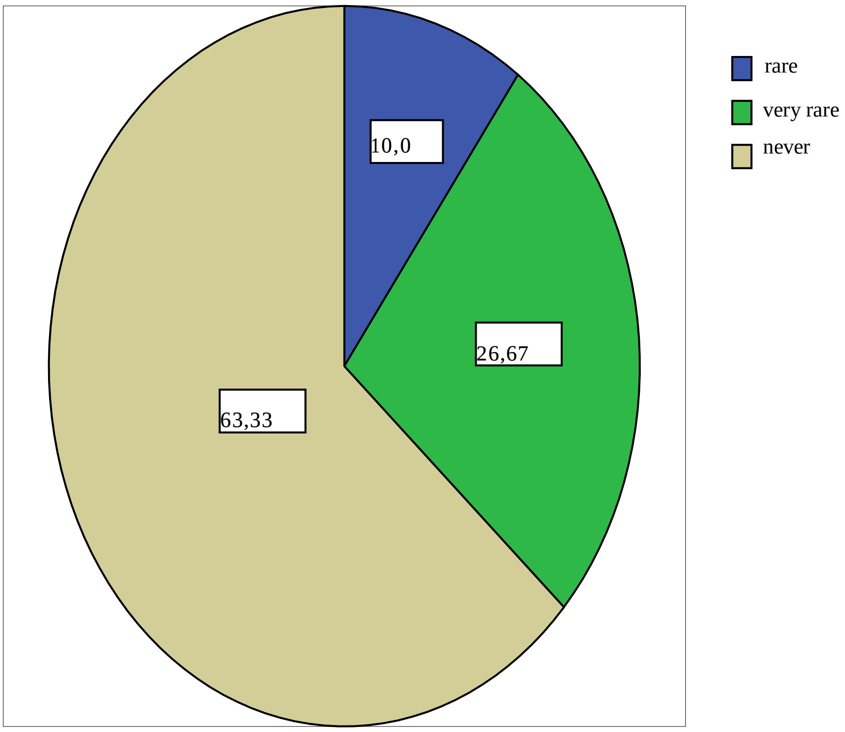
Regarding the first variable, over 50% of analysts say they delivered analytical products without sufficient information (see Figure 4), most of them belonging to the age category 31-40 years and having 11-15 years of experience.

Figure 4 – How often did you do intelligence analyses in the absence of sufficient information (percents)



On the other hand, there are quite a lot situations in which analysts do not use relevant data and information that they have available: only 63% said they always use ALL the important data in making an analytical product (see Figure 5).

Figure 5 – Did you ever deliver an analysis ignoring relevant information?



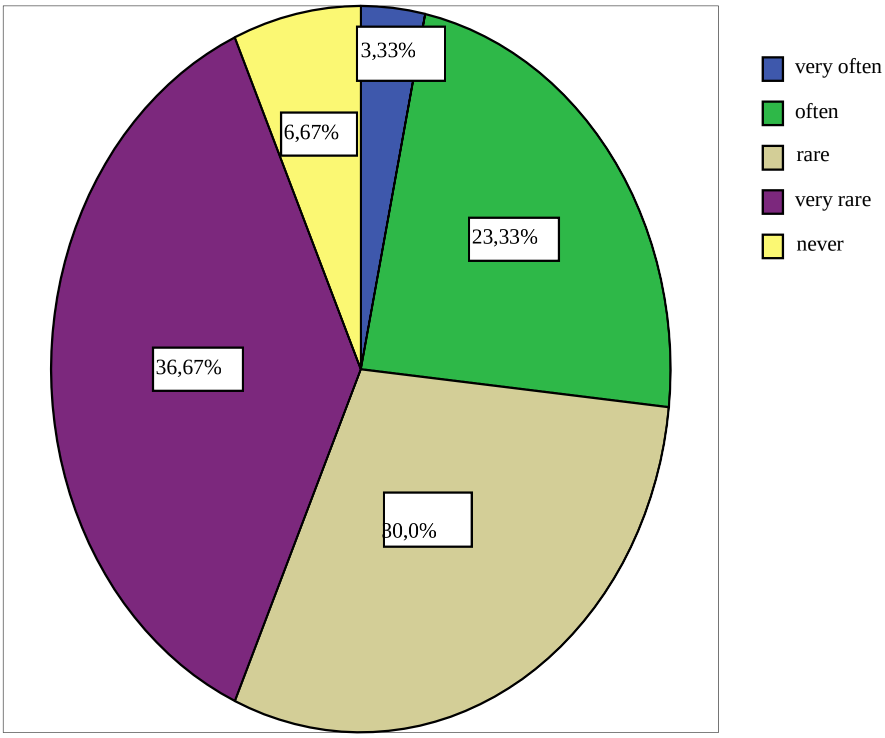
Limited expertise can be an explanation of such a situation, especially as it is reported as error-prone rather by young analysts rather than the elderly (see Table 3).

Table 3 – The role of reduced expertise in generating errors (in percent)

Does limited expertise determine erors in analytical products?	**Age**		
	21-30 years	31-40 years	41-50 years
To a less extent	-	7,1	14,3
To a large extent	22,2	57,1	71,4
To a very large extent	77,8	35,8	14,3

It seems paradoxical, but those who hypothetically have a larger experience are more moderate in saying that analytical errors have their source in the lack of expertise. In contrast, almost 80% of those between 21-30 years appreciate that things are exactly the opposite and that reduced expertise leads to errors in intelligence analysis. In addition to ignoring relevant information, over 25% of the subjects consider that another source of errors is the identification of some nonexistent causality between data (see Figure 6).

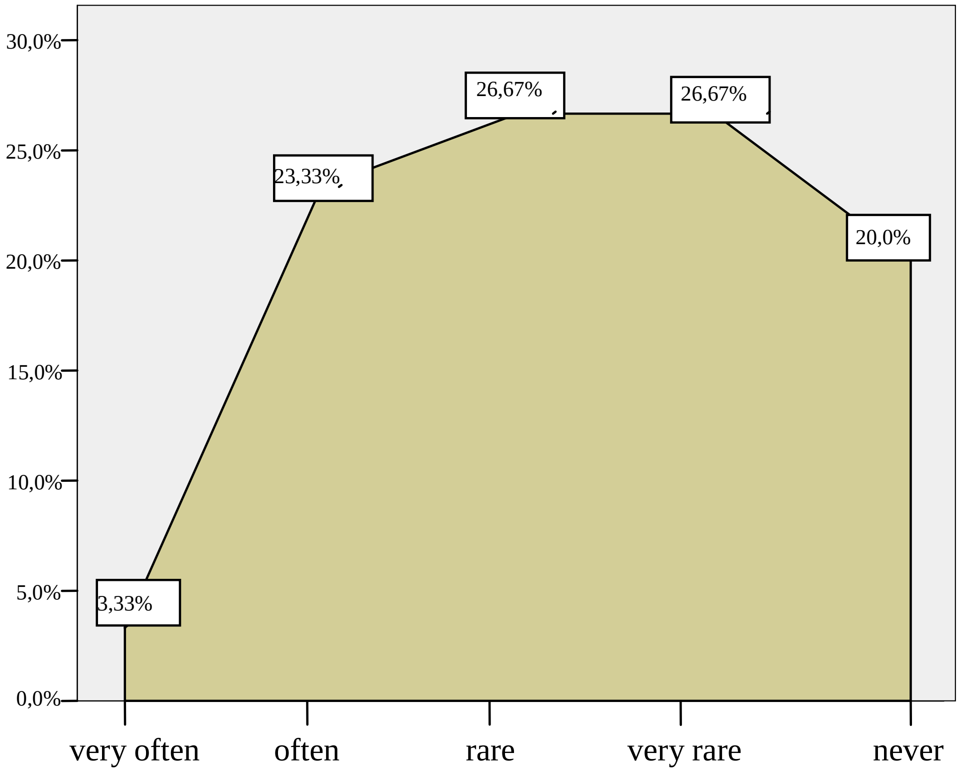
Figure 6 – Did you identify non-existent correlation between data during analysis?



This is a high percentage when relating it to the declared self-esteem of analysts, as it was previously highlighted.

Also, only 20% of analysts said they never associate negative information with a higher importance in interpreting the data (see Figure 7).

Figure 7 – Do you give more importance to negative data?



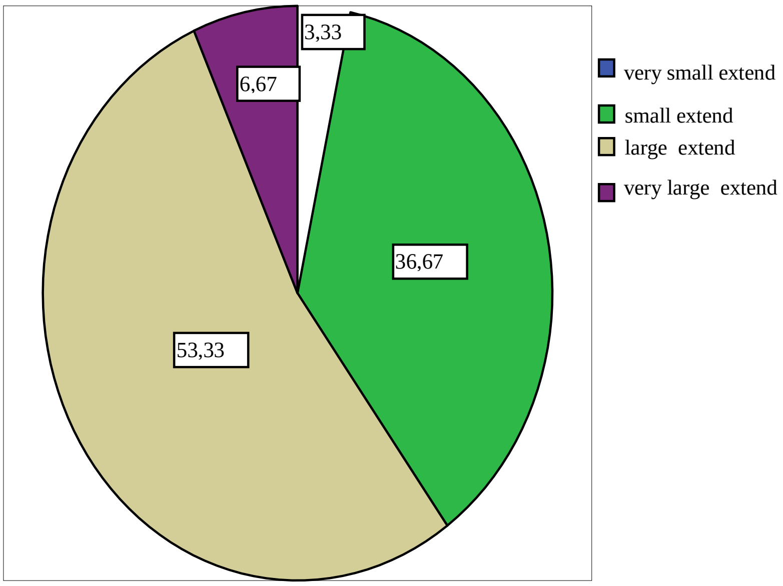
Other variables considered to generate errors by analysts are shown in Table 4, all of them scoring important percentages of agreement.

Table 4 – Variables that are generating errors (%)

Do you consider that _____ generate errors in analysis?	to a very large extent	to a large extent	to a small extent	to a very small extent	I don't know
the pressure of time	13,3	56,7	26,7	3,3	-
the lack of a mental model for analysis	16,7	50	23,3	6,7	,3
a low capacity of the memory	10	53,3	30	6,7	-
the lack of motivation	16,6	46,7	30	6,7	-
routine	3,3	43,4	40	10	,3
use of the same analytical model	13,3	33,3	43,4	6,7	,3
pressing health problems	13,3	30	13,3	43,4	-
conflictual relationship with superiors	-	43,3	23,4	30	,3
a dependance of the interpretation on data provided by the operational level	6,7	36,6	40	10	,7

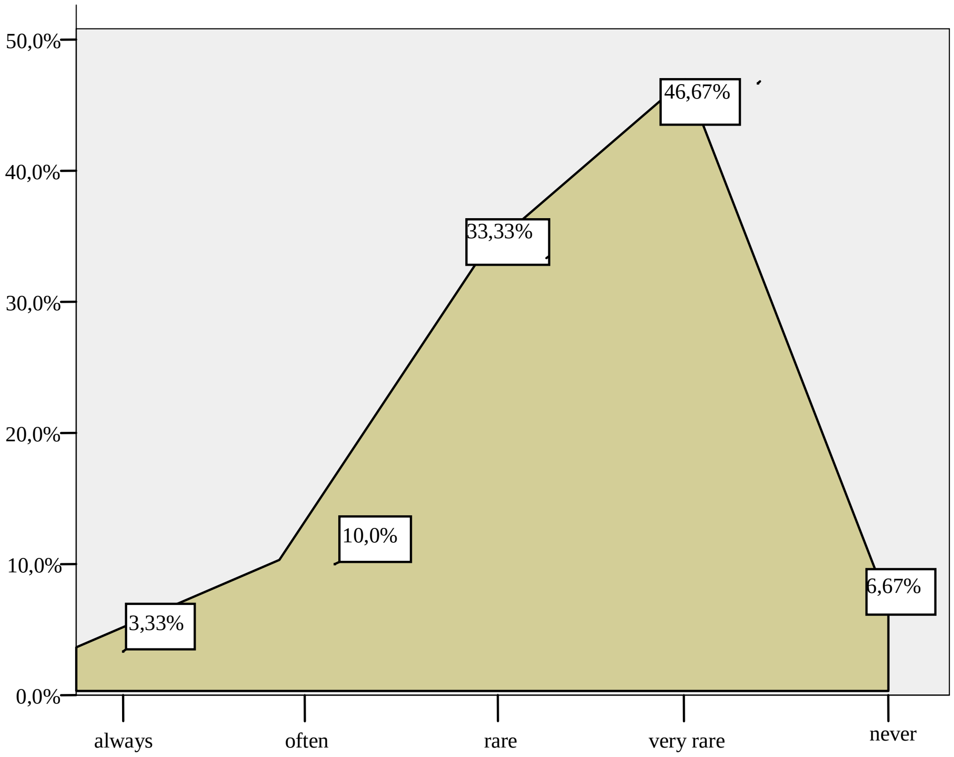
As shown before, regarding the first variable, 60% of analysts consider that they felt great and very much I am pressed for time (see Figure 8).

Figure 8 – The extend analysts felt the pressure of time?



It is also notable there is a rather large difference (20%) among those who believe that the lack of a mental model would result in errors compared to the situation where errors could be due to the systematic use of the same model of analysis. In other words, we prefer using a model consistently than not using one at all. Also, analysts realize that at least 10% of their interpretations were affected by memory deformations (see Figure 9).

Figure 9 – Did it happen to you not to remember certain data?



On the other hand, the variables that seem to have the lowest rate in generating errors are the lack of using certain methods and techniques, conflicting relationships with team members and a high concordance between team members' opinions (see Table 5).

Table 5 – Variables that generate errors (in percent)

Do you consider that _______ generate errors in analysis?	to a very large extent	to a large extent	to a small extent	to a very small extent	I don't know
the lack of using certain methods and techniques	3,3	33,4	50	10	3,3
conflicting relationships with team members	-	36,7	36,7	23,3	3,3
a high concordance between team members' opinions	10	13,3	36,7	26,7	13,3

The analysts' opinion that the lack of using analytical methods is not an important reason for errors is notable. This is correlated with the fact that nearly 85% of respondents declare they use the same method in the analysis (see Chart 10).

However, it seems that the majority use past analytical experiences when making a new analysis and base their interpretation on deciphering context (see Table 6).

Table 6 – Variables that influence analysts' work

Did it happen during your work you __________	always	very often	often	rare	very often	never
realm your interpretation on similar cases of your past experience?	6,7	26,7	50	16,6	-	
analyze data from many perspectives?	36,7	33,3	30	-	-	
analyze the context in which data has appeared?	46,7	26,7	23,3	3,3	-	

The research data also showed that the flow of information would be an important variable in generating errors and also that internal rules contribute to a lesser extent to the distortions of the analytical product. Standardization of analytical products scored very balanced scale percentages (see Table 7).

Table 7 – Variables generating errors

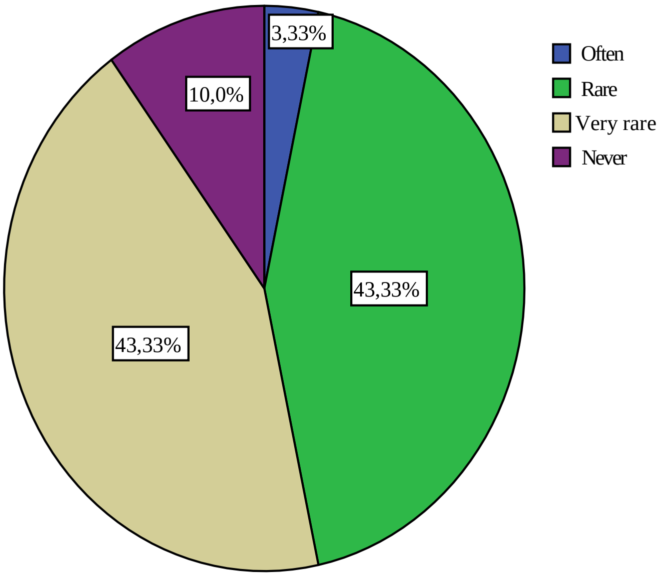
To these variables generate errors in analysis?	to a very large extend	to a large extend	to a small extend	to a very small extend	I don't know
flow of information	30	33,4	13,3	23,3	-
internal rules	3,3	30	30	33,4	3,3
standardization of analytical products	20	30	30	20	-

Analysts also specified that errors can occur as a result of other factors listed in one of the open questions. They are:

- Reduced capacity to globally understand certain developments;
- Insufficient knowledge of the analyzed issues;
- Seclusion in a particular paradigm of thinking;
- Pride (too much confidence in his own abilities);
- The unpredictable surprise;
- Unverified information;
- Unilateral information;
- Conflicting data;
- Lack of systematic guidance;
- Improper initial training;
- Orders from authorities.

Despite the existence of so many variables that could cause errors in intelligence analysis, more than 85% of respondents consider that they made few errors and 10% consider that errors never occurred (see Figure 11).

Figure 11 – Did you make errors in your analytical products?



The main factors significantly correlated with errors are included in Table 8.

Table 8 – Variables which influence /do not influence the generation of errors

VARIABLE	INFLUENCE THE GENERATION OF ERRORS	
	Significant correlation	No correlation
Pressing health problems	YES	
Insufficient data	YES	
Conflicting relationship with superiors		YES
Conflicting relationship with colleagues		YES
High convergence of opinions		YES
Lack of motivation	YES	
Insufficient expertise	YES	
Lack of an analytical model	YES	
Use of the same analytical model	YES	
Lack of using certain methods and techniques		YES
Prejudices	YES	
Low memory	YES	
Low level of intelligence	YES	
Pressure of time	YES	
Routine		YES
Dependence of operational level interpretation of data		YES
Standardization of analytical products		YES
Internal rules		YES
Analysts attribution		YES
Information flow	YES	

Therefore, it is notable that conflicting relationships with colleagues or superiors do not seem to play an important role in the occurrence of errors, and also high concordance of opinions, routine or the lack of using certain methods would decisively influence the analytical process. These factors can be grouped into a subjective area of variables generating errors. On the other hand, dependency on operational level interpretation of data, the standardization of analytical products, internal rules and analyst’s attribution are composing an objective area of variables, as analysts have less control over them.

A correlation between the shown variables and the age of respondents are shown in Table 9.

Table 9 – The influence of errors generating variables correlated with age

Variable		Age		
		21-30 years	31-40 years	41-50 years
Pressing health problems	High impact	YES		
	Low impact			YES
Insufficient data	High impact	YES		
	Low impact		YES	
Conflicting relationship with superiors	High impact	YES		
	Low impact		YES	
Conflicting relationship with colleagues	High impact	YES		
	Low impact			YES
High convergence of opinions	High impact	YES		
	Low impact		YES	
Lack of motivation	High impact	YES		
	Low impact			YES
Insufficient expertise	High impact	YES		
	Low impact			YES
Lack of an analytical model	High impact	YES		
	Low impact			YES
Use of the same analytical mode	High impact			YES
	Low impact	YES		
Lack of using certain methods and techniques	High impact	YES		
	Low impact		YES	
Prejudices	High impact	YES		
	Low impact			YES
Law memory	High impact			YES
	Low impact	YES		
Low level of intelligence	High impact		YES	
	Low impact	YES		
Pressure of time	High impact			YES
	Low impact		YES	
Routine	High impact	YES		
	Low impact		YES	
Dependence of operational level interpretation of data	High impact	YES		
	Low impact			YES
Standardization of analytical products	High impact	YES		
	Low impact		YES	
Internal rules	High impact	YES		
	Low impact			YES
Analysts attribution	High impact	YES		
	Low impact		YES	
Information flow	High impact		YES	
	Low impact	YES		

It can be noted that 15 of the 20 factors have an increased impact in the cases of subjects of 21-30 years old. Therefore, younger people are more fallible as they consider that only 5 of the mentioned factors do not generate uses of errors:

- Use of the same analytical mode
- Low memory
- Low level of intelligence
- Pressure of time
- Information flow.

Also the impact of these factors are relatively balanced within the other two age categories (31-40 years and 41-50 years), as they both have the same number of cases with low impact (8) and insignificant impact (10/9).

Therefore the most vulnerable age category to the occurrence of errors is 21-30 years. As experience and expertise are increasing, the impact of variables generating errors tends to decrease significantly. It is worth mentioning that for the 31-40 years age group the most important variable of impact is considered to be appears because a low level of intelligence and information flow while the use of the same analytical model, the pressure of time and low memory are considered to generate the highest impact in the perception of the age group 41-50 years.

Regarding the stated self-perception of the young people, there is an equal percentage (11.1%) of young people that consider they often made errors in their analysis and those of who evaluate they never made mistakes.

Table 10 – Distribution of perception of errors by age (percent)

Did you make errors in your analysis?	**Age**		
	21-30 years	**31-40 years**	**41-50 years**
Often	11,1	-	-
Rare	33,3	35,7	71,4
Very rare	44,4	50	28,6
Never	11,1	14,3	-

The distribution of perception of errors by experience revealed the following situation (see Table 11):

Table 11 – Correlation between the perception of errors generating variables and experience in their field

Variable		Experience			
		1-5 years	6-10 years	11-15 years	16-20 years
Pressing health problems	High impact	YES			
	Low impact			YES	
Insufficient data	High impact			YES	
	Low impact		YES		
Conflicting relationship with superiors	High impact				YES
	Low impact		YES		
Conflicting relationship with colleagues	High impact				YES
	Low impact		YES		
High convergence of opinions	High impact			YES	
	Low impact				YES
Lack of motivation	High impact	YES			
	Low impact				YES
Insufficient expertise	High impact				YES
	Low impact			YES	
Lack of an analytical model	High impact		YES		
	Low impact			YES	
Use of the same analytical mode	High impact	YES			
	Low impact			YES	
Lack of using certain methods and techniques	High impact	YES			
	Low impact				YES
Prejudices	High impact	YES			
	Low impact		YES		
Low memory	High impact			YES	
	Low impact				YES
Low level of intelligence	High impact	YES			
	Low impact				YES
Pressure of time	High impact			YES	
	Low impact	YES			
Routine	High impact	YES			
	Low impact		YES		
Dependence of operational level interpretation of data	High impact	YES			
	Low impact				YES
Standardization of analytical products	High impact	YES			
	Low impact				YES
Internal rules	High impact	YES			
	Low impact			YES	
Analysts attribution	High impact		YES		
	Low impact				YES
Information flow	High impact			YES	
	Low impact				YES

As shown in Table 12, the biggest number of variables that generate errors occur among people having 1-5 years of experience. For these analysts such variables with significant influence on generating errors are pressing health problems, lack of motivation, low level of intelligence or routine. At the opposite end, for those having 16-20 years of experience, the variable with the highest impact is conflicting relations with bosses and colleagues.

Table 12 – Distribution of the level of variable influence by experience

The influence of variables	Years of experience			
	1-5 years	6-10 years	11-15 years	16-20 years
High	10	2	5	3
Low	1	5	5	9
Medium	9	13	10	8

As for the low impact variables the biggest number occur for people having 16-20 years of experience while for those having 1-5 years of experience the only variable with an insignificant impact is considered to be the pressure of time.

To identify more precisely those variables that generate errors in analysis, we used an open question asking the subjects to rank the top three factors that negatively affected their analytical product. Their answers revealed the following hierarchy:

- Lack of information from open sources (12 times)
- Inaccurate data (5 times)
- Lack of depth of the topic (4 times)
- Pressure of dead line (3 times)
- Unclear information (2 times)
- Lack of information from secret sources; Wrong correlations between data; Lack of attention; Lack of experience; Use of the "known path" of doing things ; The wrong labeling of the data source.

When we scored every place of those answers (3 points for the first place, 2 points for the second and 3 for the third), the hierarchy would be as follow (see Table 13):

Table 13 – The perception of analysts regarding the hierarchy of errors generated variables

ITEM	Score	The place in the hierarchy		
		1	2	3
1. The lack of open sources data	**40**	12	2	-
2. Deadline pressure	**20**	3	5	1
3. Inaccurate data	**20**	5	2	1
4. Lack of depth of the topic	**15**	4	1	1
5. Wrong correlations between data	**8**	1	2	1
6. Lack of information from secret sources	**7**	1	2	-
7. Unpredictable events	**7**	-	2	3
8. Unclear information	**6**	2	-	-
9. Lack of attention	**4**	1	-	1
10. Prejudices	**4**	-	2	-
11. Lack of experience	**3**	1	-	-
12. Use of the "known path" of doing things	**3**	1	-	-
13. The wrong labeling of the data source	**3**	1	-	-
14. Superficiality	**2**	-	1	-
15. Rush	**2**	-	1	-
16. Tiredness	**2**	-	1	-
17. Different perspectives regarding analysis	**1**	-	-	1
18. Use of a subjective analytical model	**1**	-	-	1
19. Poor organization of computing resources	1	-	-	1

Subjects were asked to specify appropriate ways to eliminate or reduce errors in intelligence analysis. In random order, they proposed the following measures:

• Rethinking of the intelligence flow and analyst duties;

• Elimination of standardized analytical products;

• Avoiding the development of analytical products under time pressure;

• Post-factum analysis of each analytical products, using cooperation with those institutions that have contributed to the drafting of information in order to evaluate the responsibility of every structure and possible errors;

• Correctness and completeness of the information that goes to beneficiary, including the products delivered by operational level;

• Improving the quality and quantity of information provided;

• Stronger collaboration with external partners in the same field;

• Access to more type of data base information;

• Improving the quality and volume of information from secret sources;

- Specialization of analysts on one field and avoiding changing areas of expertise;
- More training for analysts;
- Better organized activity and the increasing of the role of teamwork;
- Establishment of additional filters in interpreting information to eliminate bias;
- Stimulate creativity and initiative;
- Removing templates and "wooden language"
- Develop and implementing mechanisms for using “learned lessons”;
- Motivating analysts and lowering the level of responsibility.

Finally, we tried to identify the subjective perception of subjects regarding the place and role of the analyst in Romanian Intelligence Service. Respondents consider the analyst as one of the most important employees of the institution, but also they underline that sometimes the analyst is not valued enough being seen as an marginal, additional employee, due to a distorted perception.

As subjects answered, the role of the analyst is to give value to data and transform them into meaningful messages relevant for national security. He should be the link between beneficiary and the Service as their products are designed to help decisions and to forecasts trends and future events. From this point of view, analysts see themselves as the ones who should guide / direct the gathering of information, according to information needs implied by their analysis. Moreover, they define themselves as integrators of information, but specify that they integrate information already filtered by others and this can affect the efficiency and quality of analytical products.

Conclusions

The most significant items arising from the interpretation of data proved to be those variables that have the greatest influence on the appearance of errors in intelligence analysis, which are insufficient data and information, low intelligence, insufficient expertise and the existence of prejudice.

In addition to these, other factors correlated with errors in analyses are the pressure of time, the lack of a mental model for doing analysis/ the overusing of the same model for analyzing data, a nonperforming memory, the lack of an appropriate motivation, definite characteristics of the information flow or pressing health problems.

According to the analysts' perceptions, the main ways to eliminate or reduce errors in intelligence analysis are:

- The reshaping of the information flow and the analyst duties.
- Reducing or even eliminating the standardization of analytical products.
- Avoiding to develop analytical products under time pressure.
- In order to evaluate the possible errors and the responsibility of every structure involved, analysts consider they should analyze post fact each analytical product in analytical groups that contains members of all the institutions that have contributed to achieving the document information.
- Checking the correctness and completeness of all the data included in the information flow from the very beginning of the cycle.
- The improvement of the quality and quantity of the information they receive, especially from human intelligence sources.
- The improvement of the collaboration with external experts having similar interests.
- Obtaining access to some of the operational database or information.
- The continuous improvement of analysts expertise and avoiding the change of the areas of expertise.
- A better management of the activity.
- Increasing the role of teamwork in everyday activity.
- Establishing new procedures to eliminate subjectivity and cognitive biases.
- Encouragement of creativity and initiative.
- The elimination of the "wooden language".
- Using the results of learned lessons.
- Increasing the motivation of analysts making them responsible for more decisions.

Therefore, the problems faced by the analyst are multiple and their solving depends on the efficient functionality of the any intelligence service. As analyst proved to be one of the most important employees of the institution. According to their own perceptions they consider themselves those that provides value-added information by transforming data into meaningful products relevant to the national security plan.

References

1. Irena Dumitru, *Psihologia analizei informaţiei*, (unpublished course, 2009).
2. Richards Jr. Heuer, *Psychology of Intelligence Analysis*. (Central Intelligence Agency, Washington D.C., 1999).
3. Rob Johnston, *Analytic Culture in the US Intelligence Community*. (Central Intelligence Agency, Washington D.C., 2005).
4. George Cristian Maior, "Cuvânt de deschidere", *Intelligence*, no. 13, 2008.

Cultural Intelligence and Intelligence Culture

Karin MEGHEŞAN[*]
Andreea CUCUTĂ[*]

Abstract

We live in a world of struggle - struggle for survival, for power or for influence.

Going beyond the classical competitiveness on the international scene, ideas, cultures, 'visions', are all competing against each other.

People, organizations and nations gravitate around this 'hub' which is culture. Values, system of beliefs, cognitive schemata, attitudes and behaviors, be it, individual, organizational or national, achieve meaning and can be better understood by means of culture. Values, system of beliefs, cognitive schemata, attitudes and behaviors, be it, individual, organizational or national, achieve meaning and can be better understood by means of culture.

We do not intend to dwell on the philosophical meaning of the concept, but we would rather like to focus on the analysis of the complex relationship between culture and intelligence.

We consider- from an officer and teacher's point of view- that in the future the influence of culture over intelligence will achieve a great deal of importance. We consider that efficiency and the lucrative aspect of intelligence regarding activities (in particular HUMINT), organization or product (in particular the consumer-analyst linkage) depend on culture.

We will briefly present the main points of interest (which will eventually become a further research direction) of the dyad culture-intelligence.

Keywords: cultural intelligence, operational code, intelligence failure, HUMINT, efficiency, competitiveness

Over 20 years of experience in intelligence has strengthen our belief, which we were instilled with by our parents, that if one is cultivated meaning one has vast general knowledge, one is an "intellectual" as our grandparents would call it, then one can succeed in life and can aspire to any kind of profession one might choose. But having rich general knowledge is not enough or better said it is of no use having rich general knowledge if one lacks that "je ne sais quoi" which might come naturally or eventually be educated and which of late has been given a scientific name turning into intelligence culture.

Why would an intelligence organization be interested in the theoretical development and practical applicability of a concept mostly a psychological one, the CQ (*cultural quotient*, *cultural intelligence*) which derives from such a highly debated and disputed concept ever since antiquity up to modern times, the concept of *culture*.

[*] PhD "Mihai Viteazul" National Intelligence Academy, Romania
[*] "Mihai Viteazul" National Intelligence Academy, Romania

First of all, according to Ostrom Moller[1] (without overlooking Samuel Hungtinton's "Clash of Civilizations") "the world moves from economic and technological competition toward a competition between ideas and cultures".

Secondly, the last decade has been defined by an obvious need (on all levels- individual, organizational, national and international) to effectively manage the "change".

The change and resilience to change have become key words in the context of interdependencies generated by globalization and technology.

Risking to trivialize, through repetition, Sun Tzu words of wisdom "know yourself, know your enemy and you will win all the battles" we will revisit them because we consider that they represent, in intelligence and the new types of conflicts, the "key" which will help us decrypt the link between culture and the intelligence activity.

Ultimately, intelligence culture and cultural intelligence CQ can answer certain questions such as "How can we better cope with this new world? How can we correctly perceive the reality? How can we understand each other and how available are we to actually understand and know the others? We consider that an honest intellectual approach of the two concepts, on one hand CQ on an individual and managerial level and on the other hand, intelligence culture on organizational and social level could represent the starting point of a strategy to turn a nation, a Smart Power[2] organization.

Before introducing our point of view regarding Romania in the context of dyad CQ-IC we will revise some theoretic aspects which will give us a better understanding of our approach.

Conceptual delimitations

One of the first definitions was given by P. C. Earley[3]. According to Earley CQ refers to an individual's capability to deal effectively in situations characterized by cultural diversity, and is a multifactor with cognitive (meta-cognitive and cognitive) emotional and behavioural dimensions.

Research regarding CQ has primarily focused on a business level but it proved itself useful for security enterprise- private or governmental, national or international security, as well. After all we deal with an organization which increasingly rely on alternative types of international mobility such as global managers, awareness- building assignments, commuting assignments, extend business travelling (Collins, Scullion & Morley, 2007). For a better understanding of the activity of intelligence we should rely on Roberts' CQ approach (Roberts, Kossek & Morley, 2007) " a SWAT – team, an idea adapted from special weapons and tactics units to describe highly mobile terms of experts, deployed on a short term basis, to troubleshoot, solve very specific problems, or complete clearly defined projects. Generalizing the idea of SWAT team and CQ we can assert that in the new international environment the "cultural knowledge" is essential to ensure the success of any kind of operation, be it military, intelligence or business. The "official" recognition of the importance of culture and CQ for intelligence organizations, both on operational, tactical and on a strategic level, as well, came only after the counterinsurgency operations in Afghanistan and Iraq: "cultural knowledge is essential to waging a successful counterinsurgency" (USA Marine Corps Counterinsurgency Field Manual, 2000). General Anthony Zinni, former commander of Operations *Restore Hope, Continue Hope and United Shield* concludes that cultural intelligence is indispensable: "What we need is cultural intelligence. What makes them [faction leaders and people] tick? Who makes the decisions? What is it about their society that's so remarkably different in their values, in the way they think, compared to my values and the way I think in my western, white-man mentality? ... What you need to know isn't what our Intel apparatus is geared to collect for you, and to analyse, and to present to you"[4]

Achieving success and becoming a "smart power", in a world of interdependencies, "requires a global mindset in which competing forces are equilibrated rather than one dimension being favoured at the expense of the others" (Prahalad & Doz, 1987), which according to other scholars[5], means "extending concepts and models from one-to-one relationships to holding multiple realities and relationships in mind simultaneously, and the skilfully on this more complex reality".

Returning to Ang and Early's definition (2003) we will attempt to briefly present all three dimensions of CQ since we believe that their indicators can be used to improve the intelligence activities in several fields: recruiting, training, education, analysts and recruiters training (further on we will dwell on this idea), organizational management, institutional development starting from values and system of belief building the intelligence culture. The literature mentions that the primary causes of business failure are inadequate information about the business environment and the lack of understanding of foreign cultures. We would like to extrapolate the above mentioned to intelligence failures in the context in which INTELLIGENCE could be taken either as an activity, outcome, or organization.

Cognitive dimension

This dimension of CQ represents an individual's ability to assess the similarities and differences in cultural situations in ways that allow him or her to produce culturally appropriate behaviour. This dimension refers to knowledge in general, but it is closely linked to the importance of language and the behavioural output that general knowledge can have: relationship, communication, negotiation, cooperation, respect. Culture and intelligence culture have always rooted out from the language, from speech. The language encodes images, concepts, cognitive schemata. We express ourselves and develop relationships through culture and language. Self perceptions, view of the world, knowledge are all determined by language and culture.

In the intelligence activity this dimension becomes relevant from early stages of selection, education and human resources training. In our opinion, the correct quantification (from the selection stage) of the mentalizing capability of an individual is the key to the development of an organization. In order to have a better understanding of the concept of mentalization we will use the definition given by the psychoanalysts[6]: mentalization refers to the ability of understanding one's behaviour and other individuals' as well in terms of intentional mental status – thoughts, emotions, intentions, wishes, and beliefs, ability which is usually acquired. Mentalization is imaginative because we are supposed to imagine what others might think or feel.

Perhaps the most proper illustration of the relation between CQ and intelligence in this respect is the Operational Code[7]. Used in political psychology, the operational code framework seeks to explain "the overall belief systems of leaders about the world (i.e., how it works, what it is like, what kind of actions are most likely to be successful, etc.).[8]

The attempt to correctly understand reality and the "lens" through which each individual, decision-maker, or nation sees reality was later refined by Harold and Margaret Spout in the paradigmatic paper

Man-Milieu Relationship Hypothesis in *The Context of International Politics* (1956). In the 60's the research direction opened by the two Spouts is continued by Alexander George and Michael Brecher.

In order to support the hypothesis that CQ represents a variable key to developing intelligence culture, we will resort to the excellent analysis of the operational code made by Alexander George (The Operational Code. A Neglected Approach to the Study of Political Leaders and Decision-Making, 1980[9]):

"Knowledge of the actor's approach to calculating choice of action does not provide a simple key to explanation and prediction; but it can help the researcher and the policy planner to "bound" the alternative ways in which the subject may perceive different types of situations and approach the task of making a rational assessment of alternative courses of action. Knowledge of actor's beliefs helps the investigator to clarify the general criteria, requirements, and norms the subject attempts to meet in assessing opportunities that arise to make desirable gains, in estimating the costs and risks associated with them, and in making utility calculations."

George's words remind us of intelligence analysts but they also give us the chance to highlight the importance of knowledge in intelligence activity. It is obvious for us that in the context of the subject analysed; this knowledge can only be triggered by cultural intelligence development. If at the level of a multinational manager knowledge can be obtained more or less easily (as showed in the behavioural dimension of CQ), in intelligence it has to have certain defining aspects: intelligence, intellectual curiosity, an ability to mentalize, intellectual and behavioural tolerance, open-mindedness. To have an exact image of these defining traits we will resort to the graphic scheme proposed by David Moore and Lisa Krizan[10], and, however shocking it may be, to Da Vinci's Vitruvian man (now that we reached this point, we will pose a frequent question in the intelligence communities, that still remains unanswered: how do we select, educate and train an individual so that he should have all these characteristics?)

As for the operational and intelligence code, we can say that this concept has been neglected in the literature; nevertheless, from our point of view it may prove useful not only when analysing communist or authoritarian leaders (the Cold War period, North Korea, China, Venezuela, Cuba, Iraq, Libya, Syria, etc.), leaders of terrorist organisations[11], but also when analysing national decision makers, that is the beneficiaries of intelligence products, or even when analysing competitors or partners.

Behavioural dimension

Even if it may seem the most important dimension, since after all behaviour is what can be most easily noticed, we have to say that it is based on the cognitive, affective and motivational components. Each of us (individual, organisation or nation) "sees" themselves according to our cognitive schemata, the values we believe in, intrinsic or extrinsic, cognitive or affective motivations that rule our activity.

That is why we insist on the importance of the operational code described in the literature[12] as a methodology to describe a leader's fundamental beliefs, which provide norms, standards, and guidelines for decision making; it provides insight into decision maker perceptions and evaluations of the world, and estimates of how the leader will weigh the benefits and risks of various course of action.

The behavioural dimension reflects flexibility in choosing "the most appropriate" behaviour in interacting with people who differ in cultural background (Ang, 2007). In practice, this dimension can be summarized as follows: "not imposing your own way or will but adjusting to the local culture" as a basic attitude. The behavioural dimension can best be linked to HUMINT in the field of intelligence activity. We do not believe it necessary to analyse the subject of HUMINT further on, we will only quote a renowned author highly appreciated within our courses, Henry C. Crumpton:

"The heart of intelligence, however, is human espionage. At its most elemental, spying is about understanding and influencing the scope of behaviour, from evil to exalted, and manoeuvring through this emotional labyrinth in pursuit of valuable information". [13]

Returning to the above quoted author we could state that the very core of the intelligence activity is the individual. The ability of mentalization of individuals mentioned within the cognitive dimension becomes action through behaviour. There is a transactional relationship between experiences, beliefs, emotions and behaviour (Fonagy, 2004). Among the abilities the cultural intelligence and mentalization promote we could mention some of which are considered essential in the intelligence activity:

- the ability of learning from difficult situations;
- the ability of maintaining a positive attitude through hope, initiative and acceptance;
- the ability of experiencing the authority derived from the responsibility for our own behaviour;
- the ability to have a sense of purpose and involvement in positive, motivational actions based on common values;
- the ability to communicate and problem solving;
- the ability to be flexible and have sense of humour;
- the ability to feel part of a whole, give and accept a hand in your turn;
- the ability to sympathize which allows us to see things both from our perspective and from other people's as well. (Allen, 2003)

"The successful ops officer must realize that he is not the most important part of a recruitment operation. The centrepiece of any recruitment operation is the recruitment target. The ops officer must not allow his own immediate objectives to block the aspirations of the target. The ops officer must understand that the prospective agent has a vision also. Although he may need help in expressing his needs. Uncovering and understanding the target's vision and enabling him to render an intelligence service is the ultimate objective."[14]

We believe that cultural intelligence, improved though education and training could lead to a successful career. The main ingredient of any recruitment operation will always be MICE, thus we can say that an officer who tested high scores in cultural and emotional intelligence, who possesses above average intellect, high abilities of mentalization with a vast general knowledge, is highly inquisitive, culturally tolerant will obtain better results than an officer who has a very high IQ. In other words, cultural intelligence builds an alternative framework for recruiting. We refer to Cialdini's six principles of influence (The Psychology of Persuasion) - RCSLAS – reciprocity, commitment (and consistency), social proof, liking, authority and scarcity.

The importance of the behavioural dimension of CQ is quite obvious for any professional in the field of intelligence. Personal development and ability improvement on this level do not represent a necessity only in the field of recruiting but also in the field of international cooperation in intelligence and performance management of an intelligence organization. In order to improve the ability of acquiring depth cultural knowledge managers use three types of behaviour[15]: they take a personal rather than cultural approach; they focus on cultural artifacts rather than underlying values and assumptions; and they rely on local informants rather than gaining the cultural knowledge themselves.

We will not go further with this idea, we will only highlight that this dimension refers to both verbal and non-verbal behaviour.

Motivational dimension

The motivational dimension of CQ reflects the ability and motivation to use cultural knowledge and produce culturally appropriate response (Earley & Ang, 2003). It refers to an individual's drive and interest to learn and function in situations characterized by cultural difference.

Although extremely important, the motivational dimension is difficult to quantify. Despite this, it can represent a useful tool in human resources; it can be studied and assessed during training so that the analysis could offer a behavioural schema of the future intelligence officer. The officer's identification with the mission and values of an institution, the feeling of belonging to a "cast", loyalty, and intellectual openness could measure an "individual's drive and interest".

The websites of the most well-known intelligence services offer "motivational incentives" for those who would like to pursue a career within the organization. "To establish an inspired, inclusive environment", "we recognize our strength lies in our people, we are each gifted, yet together, the sum is greater than the whole" (present on CIA's website). Yet, if one has no propensity for intellectual openness, reading, knowledge in general, if one does not accept the idea of long-life learning and self improvement, that is if one does not have the intrinsic motivation, the extrinsic is hardly enough.

In our opinion, in order to develop an intelligence culture an organization must have national and institutional human resource with a high degree of cultural intelligence. Cultural intelligence provides a baseline for designing successful strategies to interact with peoples, whether they are foreigners or co-nationals, and whether they are neutrals, friends, competitors, people of an occupied territory, or enemies. It gives the knowledge to anticipate reactions to selected course of action, and offers the possibility of a better understanding of one's self (vulnerabilities and strengths), as a premise for correct interaction with others.

Conclusions

As we are doubtlessly aware, in the military field, cultural intelligence must be built early and ready for the commander and forces prior to the start of operations. Cultural intelligence should provide the foundation of knowledge for all types of operations in foreign lands and for all levels of war, or for all types of intelligence operations in peacetime or war. Our argumentative inquiry regarding the utility of developing CQ within modern intelligence organizations did not seek to limit itself to military aspects, which were intensely debated in the last decade (perhaps due to the failure of the cultural "imperialism" promoted by the West). We focused on projecting concepts and experiences from business and military into the area of governmental homeland intelligence. Developing CQ is important for increasing the efficiency of an intelligence officer, whether he activates abroad or within the national borders, and whether he interacts with foreigners or co-workers and his own human intelligence networks.

In order to include cultural intelligence in the intelligence doctrines and strategies we should aim towards a cultural change within national intelligence community (both military and civil organizations). Human resource recruiting, education and training (either on an analytical level or operative one) should include all aspects of cultural intelligence: cognitive, behavioural and motivational. Cultural intelligence can improve the relationship between intelligence users and providers. It is an essential variable in the equation of international cooperation; it represents the baseline of any successful intelligence liaison. Cultural intelligence can help towards an organization's successful development; it can improve the flexibility and adaptability of an organization. Cultural intelligence unquestionably leads to smart intelligence, smart organization, and smart nation.

Ultimately, "the intelligence aspect relates not an intelligence discipline or source (such as human intelligence), but it is a product of analysis and evaluation of various information sources including single source intelligence".[16]

References

[1] Ostrom Moller, *apud.* Jean-Marie Bonthous, “Culture: The Missing Intelligence Variable”, *International Journal of Intelligence and Counterintelligence*, vol. 6, no. 4, 1993.

[2] *We have to highlight in this context, that even the alliances whose power has been proved in time, for instance NATO, continuously look for ways to become smart. During the Chicago Summit in 2012, the concept of Smart Defense was launched, defined as a “renewed culture of cooperation which encourages the allies to cooperate...”*

[3] P. C. Earley, And S. *Cultural Intelligence Individual Interactions Across Cultures*, (Palo Alto CA, Stanford University Press, 2003).

[4] Anthony C. Zinni, “Non-Traditional Military Missions: Their Nature, and the Need for Cultural Awarness and Flexible Thinking”, *in Capital “W” War: A Case of Strategic Principles of War, ed.* Joseph L. Strange (Quantico, VA: U.S. Marine Corps War College, 1998), *p. 267.*

[5] H. W, Lane, Distefano J. J, Maznevski M. L., *International management behaviour*, (Cambridge, MA, Blacwell, 1997).

[6] Coady, N., Lehman, P. - *Theoretical perspectives for direct social work practice.* (Springer Publishing Company, LLC, New York, 2008).

[7] *We refer here to the concept firstly introduced* by Nathan Leites in *A Study of Bolshevism*, Free Press, 1953.

[8] M. L., Cottam, Dietz-Uhler, B., Mastors, E. & Preston, T., *Introduction to political psychology (2nd ed.).* (New York: Psychology Press, 2010, p. 32).

[9] Alexander George, in Erik Hoffman, F. Fleron, *The Conduct of Soviet Foreign Policy*, (Aldine de Gruyter. NY, 1980, pp. 172-173).

[10] David T. Moore, Lisa Krizan, *“Core Competencies for Intelligence Analysis at the National Security Agency”, in Bringing Intelligence About,* Joint Military College, *p. 96 – “insatiably curious, self motivated, fascinated by puzzles, AHA thinking, observes voraciously, reads voraciously, fruitfully obsessed, makes creative connections, playful, has sense of humor, questions conventions and skills as critical reasoning, literacy, expression, foreign language proficiency, research.”*

[11] James D. Jacquier, “An operational code of terrorism: the political psychology of Ayman al-Zawahiri”, *Behavioral Sciences of Terrorism and Political Aggression*, (Routledge, 2012); Walter, S. G., “Anticipating attacks from the operational codes of terrorist groups”, *Dynamics of Asymmetric Conflict: Pathways Toward Terrorism and Genocide*, 2011, vol. 4, no. 2; Walker, S. G., Schafer, Mastors, E. & Norwitz, J. H., *„Disrupting and influencing leaders of armed groups”* in J. H. Nowrwitz (Ed.), Armed groups: Studies in national security, counterterrorism and counterinsurgency, (McGraw-Hill, NY, 2008, pp. 323-342).

[12] Marijke Breuning, *Foreign Policy Analysis. A Comparative Introduction*, (Palgrave Macmillan, 2007).

[13] Henry A. Crumpton, *The Art of Intelligence. Lessons from a Life in the CIA's Clandestine Service*, (The Penguin Press, New York, 2012), p. 36.

[14] *Ibidem*, p.

[15] Janssesns, M., Brett, J. M. *„Cultural Intelligence in global teams: A fusion model of collaboration”, Group and Organization Management, 31, 124-153.*

[16] John Coles, *USN Cultural Intelligence and Joint Intelligence Doctrine*, available at http://www. jfsc.ndu.edu

Strategic Foresight in a Volatile Environment. Look Ahead and Look Around

Olga GHEORGHE[*]
Lavinia GROZA[*]
Ioana OLARU[*]

Abstract

The paper is a condensed expression of the experience and conclusions of a group of practitioners after several years of strategic analysis addressing a volatile environment.

It discusses, in the first part, the meaning - for the purposes of this paper - of the terms "(strategic) early warning", "strategic foresight", and includes considerations on the strategic security environment, which it defines as volatile, but also increasingly complex and nonlinear.

Given these particular features of our environment, the paper dwells on the need to look ahead and also look around, constantly identifying and assessing the factors with particular relevant impact. One of these factors is the communication and information patterns. The authors consider the human environment an intrinsic indicator of any strategic volatility, although it is the most ambiguous one, compared to military factors, for example. It is easier to assess one's capabilities, but much harder – and essential – to anticipate his/her intentions and reactions.

Understanding the human environment can therefore be one of the most important means of understanding the future. It can also help the analysts better understand their limitations and better approach their fellow analysts and also, more important, the decision-makers.

The paper also takes a comparative look at the practitioners' approaches to horizon scanning and early warning, emphasizing the important and obligatory part that intelligence plays in both processes and also some of the most common mistakes analysts often fall victims to while embarking on such a difficult mission as foreseeing the future. The common understanding of a situation is, in the opinion of the authors, the "magic bullet" beyond risk assessment, early warning, foresight and even knowledge management.

In the final part, the authors argue that the solution is to constantly adapt the intelligence analysis to the rapid changes of the human environment, be it the customers' evolving needs (most of them immediate) or the new analytical methods or techniques/technologies.

Keywords: strategic security environment, intelligence analyst, strategic warning, human environment, horizon scanning, foresight, warning.

[*] PhD, University of Bucharest, Romania
[*] PhD, University of Bucharest, Romania
[*] PhD, University of Bucharest, Romania

This paper contains, in a condensed form, the experience and conclusions of a group of practitioners after several years of work addressing a volatile environment, as indicated in the panel theme, with a clear **need to look ahead, into the future.**

Few concepts have enjoyed over the recent years as much attention as “strategic foresight” and “(strategic) early warning”. There is a rich literature, originating not only with intelligence professionals, but also with academics, NGOs and businesses, which demonstrates that:

- We are definitely marked by other linguistic “fashions” than our counterparts in the late ‘80s, who spoke about “anticipation” and “indications analysis”;

- Foresight and early warning are no longer the exclusive jobs of the intelligence community;

- Many creative minds and a lot more advanced technologies – as well as sciences like mathematics – find in their environments enough incentives to embark on studying, discussing, and developing foresight methodologies.

How to look at the shifting strategic environment

One might ask, in what way does strategic foresight or strategic early warning resonate with a volatile security environment? Isn’t volatility the perfect ground for surprise, for rapid change, therefore improper for long-term anticipatory assessments?

First, some explanations of the meaning of the terms, for the purposes of this paper: **strategic early warning** relates to the identification of emerging threats – and, why not, of emerging opportunities; strategic foresight is an anticipatory assessment based on every available – and validated – all-source information, coherently describing future problems so as to help avoid strategic surprise. While early warning means identifying in advance possibly disruptive threats, foresight is a narrative that integrates accumulated knowledge and “rates” the risk/threat level and relative relations between the various threats operating in the future. Both of them provide a basis for decisions and action cognizant of the implications of the things identified, therefore represent a clear advantage for the authority/organization/customer receiving them. Insofar as they are developed in intelligence organizations, they will offer relevant knowledge that is not accessible to everyone (we all want to know things others don't know) and, hopefully, before others get the same knowledge (so as to give the owner/beneficiary a comparative advantage). As a matter of fact, there is a large part of knowledge in strategic foresight, but also a significant effort to make sense of the world in which we live as it evolves, an effort in which the quality of the analyst and of the intelligence organization play important roles.

Second, some considerations about the **strategic security environment** – which is definitely volatile, but also increasingly complex. The overwhelming majority of scholars in the field of Intelligence Analysis highlight the **new nonlinear dynamic** of the present world as a result of a wider range of drivers and trends which are shaping the global environment.

Here are - randomly listed - some of the **factors with particularly relevant impact** on the new strategic environment:

- the decline of the traditional state and the rise of new international actors, which in certain cases is doubled by internal fragmentation of the centre and devolution of power to new forces;

- the emergence of areas where the state has limited influence (e.g. conflict areas where the organized crime networks are better represented);

- globalization of illicit/elusive commodities/capital and the free circulation of technology, diseases, ideologies, religions and ideas;

- increased connectivity, which portends the bigger risk of contagion and the duplication of certain attitudes/ approaches/ actions in regions to which they used to be non-specific;

- the development of new technologies, some of which are capable of drastically transforming the current reality, occurring at the same time with a rapid process of individual technological empowerment[1].

Adding to the complexity of the global environment is **the change in the information and communication patterns**. There is an explosion of information, a multiplication of the sources of information with the significant growth of the number of individuals who generate information, in addition to traditional official, academic and media sources, and a communication-happy global population who puts special pressure on intelligence and, by way of consequence, on the decision-makers and their actions.

Much of the volatility of the strategic environment is due to the **large number of reactions to public information and communications expected from figures of authority**. This compounds the identification of valid trends to be monitored in order to develop consistent strategic foresight. There is a cascading series of tactical warning and a much shorter time between warning and decision, fast reaction being often preferred in order to avoid major disruptions. However, any tactical warning resolved is, in turn, inducing change in the major patterns being monitored to enable an advance description of a possible future.

Volatile and complex strategic environment seems, therefore, to require an increasingly more complex action by intelligence analysts in order to be able to look ahead. **Looking ahead**, focusing on some priority lines/signals and trying to evolve especially the most unexpected scenarios is not enough, however. Our experience demonstrates that “peripheral vision”, that is, attention to context is also necessary. Definitely, there are difficulties in **looking around**, in grasping the salient features of context. It is also clear that our work gets complicated if we try to involve intelligence collection in the early stages of looking around, since the effort of collecting against the vast front of events and intentions which might shape the future translates in time and resource losses. Therefore, open source information becomes the staple – and **a primary challenge of any intelligence analyst is to validate his/her open sources**.

Another challenge stems from the fact that, according to our experience, we live through a transition period, in terms of global security and stability, which is defined by imbalances in both relations between states, as key actors in the area of security, and among groups inside the various states. The often shifting balance between these actors, and especially the novel characteristics of the groups inside the various states also confront us with the need to give pride of place, in the quest for a correct assumption, to **the human environment**. People’s shared and distinctive traits, their key aspirations and dissatisfactions, their favourite ideas/ ideologies/religious creeds, their general likes and dislikes are some of the "whims" a strategic foresight paper has to take into account if it seeks to be accurate. To say nothing of the fact that, beyond being themselves humans, the decision-makers always act after clearly weighing the people's mood/feeling, whether they go with or against it.

Is intelligence adequate in strategic early warning and readiness?

Cynthia Grabo, an authority on warning processes during the Cold War and long thereafter, used to consider, in her book *Anticipating Surprise. Analysis for Strategic Warning*, that **the ambiguity of political indicators is much higher than that of military ones**. Therefore, she feared that analysts could either fall victim to a high potential concealment of intention, or be forced to resort to political indicators only in relation to what is sometimes called "the overall situation".[2] Thus, analysts were more likely to have an intuitive "feeling" that the adversary is up to something, a feeling which is not provable or even necessarily communicable to others who are not thinking on the same wave length.

In response to the problems identified by Grabo, and in consideration of the need we identified to monitor **the human environment as intrinsic indicator of any strategic volatility**, which is undeniably even more ambiguous and sometimes elusive than the political indicators, two practical measures were developed.

First, we agreed on a **list of volatility/instability indicators** over the long haul, which took as much account as possible - directly and indirectly - of the human factor and environment, containing:

- Demographic pressures
- Refugees and displaced persons
- Group grievances
- Human flight
- Uneven development

- Delegitimization of the state
- Public services
- Human rights
- The security apparatus
- Factionalized elites
- External intervention

The list of indicators was used almost 3 years ago, in combination with economic indicators, to assess the potential future disruptions in a number of 13 countries in a broad area that witnessed “the Arab Spring”. While writing these conclusions, we found out that 7 of these 13 countries followed the instability pattern – some of them never emerging from it, others knowing a relapse after a brief change of paradigm. Moreover, of the remaining 6 countries 4 have very fragile security prospects, a mere aggravation of 2 indicators being likely to throw them off course.

As you may see, **looking around seen primarily as the need to understand the human environment in order to anticipate the nature of future threats and to avert/mitigate their effects is not necessarily simplifying the list of indicators**. If we take into account the fact that we already see, in this transition period, failed and failing states which are in danger of collapsing, continued ethnocentric, sectarian and religious conflict often spanning whole regions, and crossing nation-state boundaries, socio-economic threats like health risks, the spread of diseases and high cost of medical aid and food security, we fully understand the rationale for the unprecedented development of risk assessment, horizon scanning, early warning and foresight methodologies and units in a large number of states and international organizations.

A UK PMSU Background Paper of February 2005[3] argued that **prevention is cheaper than reacting to crises once they have emerged**, and preventive action would be cost-effective even at a 25% successful identification rate for emergence of violent conflict. This explains, without need for further quotations from various authors, why we have an abundance of how-to material and – should we ask for best practices – there certainly would not be any shortage of proponents.

While Yiu and Mabey did not necessarily reflect, at the time, on agreed UK policy, **the key elements of the process** which they presented do appear in most of our sources, and we do share some of them, such as:

- clarity of assumptions and of data sources;

- comprehensive use of sources and approaches;

- contestable approach using a structured process and assessments produced by different methods and sources;

- comparable assessments between different countries and regions.

However, when they say that there is no magic bullet to producing these assessments, in particular because intelligence is required to strengthen its role as support to decision from the short (1-2 years) and medium (5-6 years) to long term (10-15 years), it is our opinion that **the "magic bullet" is beyond risk assessment, early warning, foresight and even knowledge management**. It is the *sine qua non* of an effective foresight, and consists of **the common understanding of a situation** (global, regional or country-specific) by all the analysts involved, irrespective of their respective professional ambitus and expertise, and also a shared understanding of the situation between the analysts involved in foresight and the decision-makers to whom they offer support.

There is a debate whether horizon scanning, foresight, warning are natural functions of intelligence. In light of our proposition relative to the common understanding of the situation, by both intelligence, domain experts and decision-makers, we consider that in order to offer customers an over-the-horizon and big picture of the future **intelligence is the obligatory ingredient of the work process**. The intelligence organizations hold a lot of knowledge, accumulated and validated in time, not only about hard security issues but also about political, demographic, economic, technological, social and environmental ones, which also translate in a historically grounded understanding of the countries/areas/actors likely to turn any of these into forces of change.

We state that **the future has to be mapped because it will become the present and the future risks will become the present threats**. In so doing, what best opportunity than to put to use the accumulated knowledge about how our present and the current risks developed? Certainly, all of us, no matter how young, can recall from our (not so) recent past, some big discontinuity that has resulted in part of our current conditions.

To make the most of its treasure trove, intelligence analysis must beware the recurring problems already identified by Grabo in warning analysis, and also to make sure that their partners in collection, as well as customers, are immune to similar pitfalls expecting them in their own acquisition processes:

- inadequate recognition of emerging threats, particularly those of low probability but potential great danger;
- a consequent inadequate collection against such threats;
- breakdown of communication between collectors, analysts and agencies;
- failure to heed the views of the minority;
- lack of proper resources and time to address anomalies in scenarios;
- vulnerability to deception[4].

Another key element, especially in the present day complex and volatile environment, as we described it earlier in this paper, is **the need to make sense while the analysts have an oversupply of information**, often ambiguous and conflicting. This is yet another reason for our plea to have analysts, experts and decision-makers pool their knowledge and insight and develop a common understanding of the situation. Although striking an indicator out of the monitoring list can result in overlooking a potential future threat, it is less damaging than working from conflicting baselines/pictures to reach totally divergent end results.

As we remember, Yiu and Mabey considered a 25% ratio of success as clearly cost-effective, especially when working over the long-term. Therefore, **possible futures - especially the more distant - and anticipating them give new meaning even to mistakes**.

But what other mistakes do we make? Our recurrent “post-mortems” (there have been a lot of crises, these past years) determined us to largely subscribe to **the list of current errors** put forth by Schwartz and Randallv[5], with some amendments *(italics below*) deriving precisely from the distinction between their intelligence and foresight efforts being placed in a business context, while ours developed in an intelligence context:

- establishing the wrong goal – *we discovered that some sort of “penalty” was attached when analysis did not make the most accurate prediction. In exchange, our correct performance indicator should have been to have formulated the right questions, and obviously the most appropriate answers to support the best strategic decision and effective actions relative to our security interests and priorities*;

- searching the immediate answers because the customer wants to know **now**. *To escape this trap we have developed, in time, a two-tier approach to certain issues/indicators, which are dealt with both under urgent need commands, and as emerging threats*;

- looking in the wrong direction because we can’t figure out what really matters and what is ballast. *The antidote, of course, is the close connection between intelligence analysis and the real needs of the customers, which allows for certain biases, especially connected to the immediate evolutions/implications, to be counterbalanced by continued low-intensity focus on those with higher impact, capable to irremediably change the environment;*

- using the critical approach (Is it possible for X to happen?) rather than the creative one (What if x?). *The effect of such an approach is a false anticipation, equivalent to reactivity instead of proactivity. To encourage the creative approach we encouraged the listing and examination of all scenarios, regardless of their probability, since the impact of less probable scenarios is as critical as the probable one's;*

- lack of systematic approach because it is difficult to correlate different sources. *To mitigate the effects of this pitfall we made a clear distinction as to the use of open source/all source monitoring/analysis at the different stages of an issue (emergent, persistent or urgent);*

- the predilection for the dominant opinion, largely embraced by the majority. Because of this bias the relevant signals are ignored. *Luckily, especially when we deal with possible futures beyond the 10-year threshold, there is seldom a clear majority, dominant opinion...As for how we "blunt" our biases, cooperation between analysts looking at the same region from different professional angles, discussions with partners and occasionally customers, as well as exercises in which analysts with the same training, but different tasking (therefore with no foreknowledge of the region) participate are contributing to a constantly better awareness of the pitfall.*

The quest for the "perfect solution"

The security environment's extreme complexity and – ever more frequently – volatility requires foresight and warning intelligence to evolve constantly and to become an adaptive system equally complex, capable to identify patterns and develop multiple watch-points, the use of the open sources and multiple indicator sets being crucial. For those of you who still remember British politician and prime-minister Harold Wilson, a quote: "*He who rejects change is the architect of decay. The only human institution which rejects progress is the cemetery*."

It is an easy task to assess the enemy's capabilities, but the key is to predict its intentions. There is the risk of overwarning, but it must be kept in mind that the political decision-makers' actions are costly in terms of time and resources. Also, **early warning is just the first part of the equation, the other one being early response**.

The analyst should understand the policy-maker's need for information about what is going to happen in the immediate future in order to have enough time to mitigate the risks (**the tyranny of current intelligence**). The customer expects from intelligence asymmetry: he wants to know things others don't, or before others do[6].

On the other hand, the customer should be helped to understand that intelligence involves considerable uncertainty and ambiguity and give **appropriate indications and feedback**, respectively, concerning what he/she actually wants to be warned about.

Since no intelligence enterprise is good in itself and for itself, the relationship with the customer/decision-maker is the linchpin for success. Again, in addition to the common picture/common understanding that we have advocated all through the paper, we would like to mention Grabo's considerations about the "climate of opinion"[7] which illustrates part of the difficulties the customer has to reconcile while doing his/her part of the job: "[...] *the national leadership in the end is responsive to public opinion, it can also do much to shape it, and in the short term may even run counter to it on international issues*".

Apart from this key relationship which is currently evolving between intelligence analysts and their customers, **strategic foresight/warning should never remain a simple surveillance exercise**. It must detect events that could be precursors to threatening acts and, over the long haul, look ahead for threats non-identified yet. In this dual quest there is a need for analysis to be both systematic and creative (Schwartz and Randall indicate this challenge in their paper). There are many models or solutions put forth in different contexts and publications[8], but the one solution that we favour is to **adapt the intelligence workforce to the current strategic environment challenges**. This means designing a strategic analyst career path which is long and consistent enough to enable **appropriate training** as to the methods. Also, to hire creative thinkers, with motivated expertise and who should be offered **task continuity**. Where foresight is implied, we need professionals with deep cultural understanding, customer-focused, capable to "look outside-in and inside-out" (which means that they can see both risks/threats outside and vulnerability inside their organization/country), but also with sufficient external exposure to best practices in various domains, including extra-governmental and academic.

This does not mean that we are exempt from future surprises. But, as the panel theme runs, adaptive intelligence is the key word, and if it is ready to recognize a likely future, and, most importantly, react to it, it will, most certainly, also **recognize the future human environment it itself needs to develop to be able to fulfill its mission**.

References

[1] Magdalena Adriana Duvenage *Intelligence Analysis in the Knowledge Age. An Analysis of the Challenges facing the Practice of Intelligence Analysis,* thesis at Stellenbosch University, March 2010, accessed 20 August 2013 at www.scholar.sun.ac.za

[2] Cynthia M. Grabo, *Anticipating Surprise. Analysis for Strategic Warning* (University Press of America, Inc., 2004), p. 78.

[3] Chris Yiu and Nick Mabey "Countries at Risk of Instability: Practical Risk Assessment, Early Warning and Knowledge Management", *PMSU Background Paper*, February 2005, p. 1 accessed 21 August at www.pdf.aminer.org

[4] Scott K. Swanson *Indications & Warning Post 9/11: New Strategies in Intelligence* accessed 20 August 2013 at www.fas.org

[5] Peter Schwartz and Doug Randall "Ahead of the Curve: Anticipating Strategic Surprise" *How to Anticipate Forcing Events and Wild Cards in Global Politics, editor Francis Fukuyama, The Monitor Group*

[6] Richard Marrs, *Early Warning Signals: A Conversation for Exploration - Part 1,* accessed 20 August 2013 at www.altamong.com

[7] Cynthia M. Grabo, *op. cit.*, p. 157.

[8] Of which we randomly selected Wolfberg (Wolfberg, Adrian. 2006. *Military Review*. July-August 2006, p. 36) who proposes a mindset in which the analyst applies both intuitive and structured methods, that there are multiple, interrelated mysteries that must be solved simultaneously across a broad spectrum of intelligence requirements using many possible explanations or overlapping pieces of explanations. This mindset will assist analysts who are confronted with mysteries (and not puzzles) for which they cannot identify the problem, because they are too vague or there are too many.

A Wheel Is Still a Wheel. The Role of Intelligence in an Evolving Threat Environment

John BUCKLEY[*]

Abstract

In a multi-polar world, where, increasingly, networks, non-state actors and coalitions are challenging the state's role in managing threats, the argument is made that the mission of intelligence is changing. This paper seeks to challenge that argument and does so in two ways. Firstly, the paper argues that it is not the concept of intelligence that has changed but the lack of understanding of what intelligence is and its function in a civil society. Secondly, the paper will argue that the fundamental methods required to address evolving and changing threats are already in existence, and that if there is a failure, it is on the part of some involved to understand and delineate their role in combating these threats.

Keywords: intelligence, changing threats, integrated approach

Intelligence in context

It could be argued that the world was once a simple place. A more accurate statement may be that our view of the world, and the view of most others in it, was that it was a simple place. The world has not changed but the inhabitants of it are now in a position to view the world in all its complexities. Not only are they much more aware of what is going on throughout the world, but they can exploit that knowledge, to further their goals. The central factor that has brought this change about is information technology in all its guises. It is only in the second half of the twentieth century that televisions became readily available to homes and these were mostly in modern western democracies. Even these countries had to wait for the eighties for computers to start to appear, for the nineties for the internet and mobile phones to make an appearance and it is only well into the 21st Century that this technology has gone global. The advent of all this technology has meant that the inhabitants of planet Earth are now confronted, on a daily basis, with issues that less than thirty years ago they would never even have been aware of, yet these same inhabitants often cling to the idea that their lives should go on as before. It is in this multi-polar context that we seek to examine the role of intelligence in responding to the risks that are present, but as Gross (2010:1) remarks:

[*] HSM Training and Consultancy, Ireland

"The contemporary explosion of knowledge or the observation that our current age is the beginning of a knowledge society thus has a little remarked on corollary: new knowledge also means more ignorance. Thus, surprising events will occur more frequently and become more and more likely. If this is the case, handling ignorance and surprise becomes one of the distinctive features of decision making in contemporary society. The challenge in dealing with surprises lies in the fact that they lie beyond the spheres of probability and risk."

James Woolsey, the former director of the Central Intelligence Agency, commenting on the fall of the Soviet Union refers to many of the problems the changing environment has created for those involved in intelligence:

We have slain a large dragon, but we now live in a jungle filled with a bewildering variety of poisonous snakes. And, in many ways, the dragon was easier to keep track of.

Speaking with regard to the complexities encountered by the various customers for intelligence Richards (2010a:44) provides an extensive list of possible threats that have to be faced:

Military threats are still there, but they are now supplemented with complex transnational threats such as terrorism and organised crime, human security factors such as threats to populations from pandemics, natural disasters and climate change.

However, it should be recognised that of the many risks that governments have to manage, a significant number of them lie outside the remit of intelligence activities. Identifying and managing these risks lies not with intelligence agencies and law enforcement but with other government departments such as health care, with sociologists, and scientists from academia and in some cases, with the private sector. How much assistance those involved in collecting intelligence can provide to address some of these broader risks is hardly worth debating, given the limited resources they already have to address other more pressing and relevant risks. It is hard to see how the skills and knowledge of intelligence practitioners can be used to address the risk of a natural disaster or a pandemic, save where the pandemic originates as some form of bio-terrorism.

Defining intelligence

If one is going to discuss a concept it is always beneficial to have clarity with regard to what is being discussed. As Warner (:3) states: "Without a clear idea of what intelligence is how can we develop a theory to explain how it works." Yet, a definition of intelligence remains elusive, while at the same there is the perception of a shared understanding. Grieve (2008:10) speaks of "labels widely employed but variously understood" and an "illusionary perception of consensus", while Lowenthal (2006:123) in discussing the ambiguities that arise in intelligence refers to what he calls "lowest-common-denominator language" and describes these as "an attempt to paper over differences with words everyone can accept."

To attempt to obtain some degree of clarity Lowenthal (2006) adopts an approach that views 'intelligence' in three ways: as a process to get a product, the product resulting from that process and the people responsible for the process. While there is a degree of truth in all these aspects they do not provide a clear understanding of what intelligence is. McDowell (2009:11) defines intelligence as "processed information" and while this is both succinct and accurate it requires some further clarity (the devil being in the detail surrounding the process involved). Harfield and Harfield (2008:55) provide the same definition: "Intelligence is processed information." In addition, they state the purpose of intelligence as being to "inform decision making," an addition that undoubtedly has significance when considering the application of intelligence in the context under discussion. In order to be clear of the intended scope of the intelligence function and to try and limit the ambiguity involved the definition used in this paper will be:

Intelligence is a product, derived from the movement of information through an agreed process, which is created for the purpose of assisting in the prevention or investigation of crime and/or for the purpose of national security. (Buckley 2013)

The people who create intelligence are law enforcement, the military and the various intelligence agencies and the process involved can, for the most part be adequately explained by a model known as the 'intelligence cycle'.

Intelligence cycle

The much maligned intelligence cycle is a model that is widely recognised by most with any experience in working or studying intelligence management. Like all models it is not perfect and its worth has been subject to extensive scrutiny by academia. (Phynthian, 2013; Aldrich, Andrew, and Wark, 2009) Despite much of the criticism of it, its utility as a road map to guide practitioners through the collection and processing of intelligence is obvious to most working with intelligence. Its relative simplicity has an undoubted appeal and, if one does not take an overly semantic approach to each and every stage of it, then it allows all involved to see more clearly what their role is in managing intelligence. As a simple explanation of a step by step process, moving from identifying requirements to collection, to analysis, to dissemination and exploitation, it is sometimes difficult to see why so many are keen to use the intelligence cycle as a punch bag.

It is for governments to direct agencies as to against what threats intelligence should be collected and it is for those who have expertise in intelligence collection, to provide what they have been told to provide. Ultimately, it is for governments to decide what happens as a result of the intelligence collected. However, sometimes there is reluctance on the part of intelligence collectors to share the intelligence they have collected with other partners. Gray and Slade (2008), in discussing the intelligence cycle and its application to counter terrorism, provide an example of one of the problems encountered in joint ventures between law enforcement and the intelligence community:

The reality that US intelligence agencies do not share information well should come as no surprise – it is both the direct and unintended consequence of policymaker action.

The "policymaker" they are referring to is the government. While those involved in the intelligence function are often blamed for failing to combat threats effectively, it is more often than not a lack of clear understanding by policymakers, of the nature of intelligence and how it should be managed, that is the root of a problem.

Role specification

A lot of the problems that relate to managing the type of risks facing a nation is a lack of clarity about what the role of various participants is. To help illustrate and define roles a simple model (Figure 1) may be of assistance, though some may take delight in critiquing it for over simplicity. At the centre of the model is government and, whether a citizen voted for them or had them imposed upon them, it is the primary function of government to protect the nation. To support that function the government can call upon the intelligence agencies, law enforcement, academia and the private sector for an integrated approach.

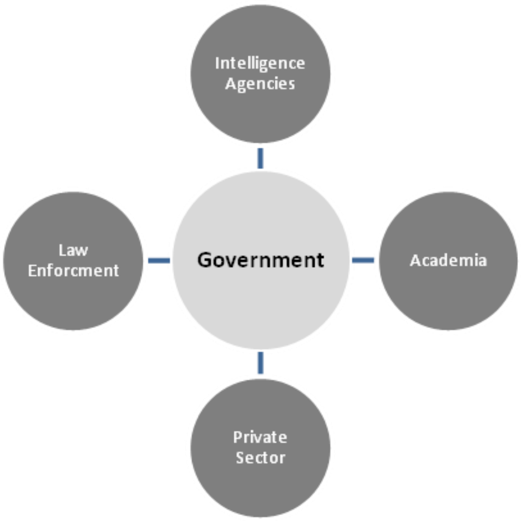


Figure 1 – An integrated threat approach

Government role

In some countries governments, have advanced in attempting to identify and stating the threats that the nation is facing; for example, the preparation of the United Kingdom's 'national security risk assessment' (Richards, 2010a), in which the government has tried to identify threats to the nation's security likely to be faced in the next twenty years. A simpler document exists in the United States in the form of an annual threat assessment (Fingar, 2011). Such documents help give clarity to the other partners involved with regard the direction that the government believe they should go in. Clearly stating risks makes it significantly easier for all to understand the sort of activities they should be undertaking. Without such direction it is easy for others to waste time and resources collecting huge amounts of data that has little or no relevance. Discussing this problem with regard to intelligence Phythian (2013:3) comments: "The key point here is that the combined potential of covert and open sources is staggering."Governments must decide what they want those with the expertise in intelligence to spend their time and the taxpayer's dollars on.

There are undoubted problems with government taking the lead in such a venture. These problems are broad in nature including everything from a lack of understanding of the intelligence function to using intelligence to advance their own political agendas and to court the favour of voters. It would not be the first time that a government acted out of their own self interest, despite overwhelming evidence supporting a different course of action from the scientific community, or the best advice given by those collecting intelligence. It must be acknowledged that sometimes it cannot be easy for government to make decisions especially when there is conflicting evidence and advice. Nevertheless, those with the collection expertise need direction from government and it is not always easy to get the clear direction that they require. As Turner (2006:4) comments:

"True, it's not easy to know what political leaders want or need, mostly because they themselves do not know."

There is no doubt that the task for government of combatting all the known risks is immense, let alone in identifying new and emerging risks, but governments have another problem. This stems from the ready access that citizens now have to vast amounts of often conflicting information available in the knowledge society. How government manages citizen's concerns and expectations is not an easy task (Innerarity, 2012).

The role of intelligence agencies

A clear understanding of the intelligence function is needed if government is to gain maximum benefit from the expertise of intelligence agencies. Discussing the purpose of intelligence, Gill and Phynthian (2012:1) comment:

Our starting point should be to recognise that intelligence is a means to an end. This end is the security and even prosperity of the entity that provides for the collection and subsequent analysis of the intelligence"

Johnson (2007:2) writing from a USA gives a frank view of the intelligence function:

In short the world has secrets that the United States and other nations may want to know about especially if they threaten the safety and prosperity of their citizens and foreign allies. Sometimes stealing this kind of information is the only way to acquire it.

He continues (2007:5):

The bottom line is that good governmental decisions rely on accurate complete unbiased and timely information about the capabilities and intentions of other nations, terrorist organizations and subversive groups.

Lowenthal (2006:2) is also clear with regard to the role of those working in intelligence:

The foremost goal of any intelligence community must be to keep track of threats, forces, events and developments that are capable of endangering a nation's existence

He (2006:255) continues:

Governments have intelligence services because they seek information that others would deny them.

The intelligence function is not about research or discussion - it's about getting material the government needs to make a country safe and to help it prosper. That material is hidden by those who would seek to harm the nation. The idea, held by some, that all an intelligence agency needs is a good search engine and everything government needs can be dragged from the internet is misguided and shows a lack of understanding of the skills necessary to collect intelligence effectively.

While intelligence collection is a function of government those involved need to be careful that they do not become puppets of the government. Failure to remain objective, despite government agendas can cause irreparable damage to the credibilitity of intelligence agencies and the profession as a whole. No better example of this is the damage that was caused with regard to intelligence reporting on weapons of mass destruction prior to the Iraq war.

The role of law enforcement

Dealing with varied and changing threats should be nothing new for law enforcement and gathering intelligence to meet these threats is already standard practice for many law enforcement agencies. The concept of intelligence led policing (UK Government Home Office. 2000; Peterson 2005) has been present for many years now and is well entrenched in many law enforcement agencies. Agencies, such as Interpol and Europol, have already structures in place at least to begin to combat the threats such as human trafficking that are posed by transnational crime. Undoubtedly, there is a need to research how well these existing arrangements function and if and how they can be improved. Furthermore, while their may be structures in place for the exchange of investigative information, arrangements for intelligence sharing require development. While the problems of intelligence sharing across international boundaries may be well known by those working in these areas, there is undoubtedly a dearth of empirical evidence to support the views held by practitioners. It could also be argued that many law enforcement agencies simply do not have the resources made available to them, by their respective governments, to meet threats that have limited impact within those nations.

The role of academia

There is no doubt that the academic community has a significant role to play in assisting government in managing many of these risks. The scientific side of academia has both the knowledge and research capability, arguably unimpaired by commercial bias, that can contribute a significant amount to the knowledge that governments need, to address risks such as that created by global warming or pandemics. The role of the academic community when it comes to intelligence studies is arguably much less well articulated. The difficulties for the academia in relation to studies involving intelligence are well at least in part articulated by Warner (2009:17):

Intelligence this by definition resists scholarship. As a result the study of intelligence is not one field but two. Intelligence studies have been conducted one way on the "outside" with no official access to original records, and another way on the "inside" where a few scholars have intermittently enjoyed sanctioned (if not always complete) access to the extant documentation. The differing natures of the source materials available to scholars on the inside and the outside, naturally have caused the academic researchers and students of intelligence to work differently from official historians and investigators in the employ of the state.

The need for more literature has been long recognised. Sherman Kent, viewed by many in the United States as the father of intelligence analysis, commented (1955) on the importance of creating a body of literature regarding intelligence that would assist in developing intelligence management as a profession:

Intelligence today is not merely a profession, but like most professions it has taken on the aspects of a discipline: it has developed a recognized methodology; it has developed a vocabulary; it has developed a body of theory and doctrine; it has elaborate and refined techniques. It now has a large professional following. What it lacks is a literature. From my point of view, this is a matter of greatest importance. As long as this discipline lacks a literature, its method its vocabulary, its body of doctrine, and even its fundamental theory run the risk of never reaching full maturity.

Unfortunately, while there is now a significant body of literature written on intelligence it could be argued that little of it is of any real use to those working in that arena on a daily basis. What academia has to decide is for whom are they researching and who their readers are. If they merely want to contribute to a perception of history or share their intellect with fellow academics then the style and content of much of what is presently written will suffice.

However, if academics want their research to be of practical value to those directly involved in intelligence collection and for intelligence customers, then there is an urgent need to reconsider the direction of much of the research and language used to articulate it. As Rossman and Rallis (2003) comment:

The goal is to present your findings in such a way as to maximize their usefulness to readers.

Quite simply, most involved in the real world of intelligence, struggle to *understand* what is being articulated in many academic papers, and even where understanding exists, the question of *relevance* often arises. So much of the work produced by so called intelligence studies has little or no worth to those charged with gathering intelligence or protecting citizens from harm. Adding to this problem is a perception by those in intelligence of unfair criticism being levelled at them, by academia. Betts (1978) provides a word of caution for academia researching in regard to intelligence failures:

Intelligence failures are not only inevitable, they are natural. Some are even benign (if a success would not have changed policy). Scholars cannot legitimately view intelligence mistakes as bizarre, because they are no more common and no less excusable than academic errors. They are less forgivable only because they are more consequential. Error in scholarship is resolved dialectically, as deceptive data are exposed and regnant theories are challenged, refined, and replaced by new research. If decision makers had but world enough and time, they could rely on this process to solve their intelligence problems. But the press of events precludes the luxury of letting theories sort themselves out over a period of years, as in academia.

Before identifying where academia can be of most benefit to those working to create intelligence, it may be helpful to identify what is not required. The only thing intelligence world needs less than another post graduate dissertation on intelligence failures relating to Pearl Harbour or the Bay of Pigs is another verbose paper written by an intelligence studies professor, populated with research jargon and with a 'catchphrase' stolen from another discipline then misapplied to the world of intelligence work. Too often the only thing that such papers achieve is to drive a deeper wedge between those involved in intelligence work and academia, with all academic work then mistakenly being labelled as having no practical worth. This is detrimental to all. What those involved in intelligence work do need, is much more research that enables them to function more efficiently. If academics want to contribute they need to keep their work real and relevant to those engaged in collecting intelligence. For example, often those involved in intelligence collection are required to provide insight into the minds of those threatening the national security of a country but they do not have the knowledge to make good judgements in this regard. There is a clear need for academia to research and develop methods to assist intelligence collectors in such a role. Some academics have identified the need for research around the psychology of intelligence analysis (Richards 2010b, Heurer 1999) and as Wirtz (2007:32) comments on the utility of this type of research:

Scholars have turned to human cognition and psychology to understand both intelligence successes and failures. Scholars have identified cognitive biases that can impede analysis.

The challenge for academia is arguably to make their work more relevant to practitioners as opposed to relevant to other academics.

Private sector

The involvement of the private sector is essential if many of the threats that exist are to be effectively combatted. Not only will they often be the target of these threats, for example in the theft of commercially sensitive material and intellectual property but they are potential victims from both terrorism and illegal cyber activities. In many circumstances they have an incentive to assist the public sector and are in a unique position to provide assistance. Furthermore, there is a role for the private sector in identifying and managing risks relating to the wellbeing of both nation states and citizens. They often have expert knowledge of the risks that are present and can take significant steps to mitigate those risks. However as O'Hern (2008:64) notes there can be a conflict:

Because a nations political position may be detrimental to the financial position of some of its citizens, owners of stocks and bonds may have much less interest in politics than what benefits their portfolios.

Where there is a shared interest those in the private sector are important partners in working with government, law enforcement and intelligence agencies both in developing new products to assist those agencies and in mitigating the risks that may be present. Examples of effective private/public partnerships are often found in crime prevention and in counter terrorism. Government bodies such as some Fusion Centers in the United States and the National Counter Terrorism Security Office in the United Kingdom are both examples of private and public bodies working to address the threat of terrorism. On the negative side recent court cases have highlighted where the private sector has circumvented money laundering regulations, aimed at preventing crime and terrorism, because of an overriding commercial interest. One must always treat the views of the private sector with some scepticism for if there is a profit to be made that profit is likely to be foremost in their minds.

Conclusion

There is a misplaced perception that many so called intelligence failures could have been avoided if only those involved had done something differently, the inference being that what went wrong could have relatively easily been avoided. However, much of the criticism aimed at those involved in intelligence is often littered with half-truths and conjecture and viewed with a hindsight bias (Hoffrage and Pohl 2003). As Betts (1978) points out:

Observers who see notorious intelligence failures as egregious often infer that disasters can be avoided by perfecting norms and procedures for analysis and argumentation. This belief is illusory. Intelligence can be improved marginally, but not radically, by altering the analytic system. The illusion is also dangerous if it abets overconfidence that systemic reforms will increase the predictability of threats.

Undoubtedly there is a need for those working in intelligence to change how they do things. It may well be that their culture of secrecy and their reluctance to share what can be shared contributes to the perception that they are incapable of changing practices to meet a changing world and their inability to learn from past mistakes. One only has to compare the similarities in the huge security compromises involving Bradley Manning and Edward Snowden to question the ability of some involved in intelligence to learn from previous mistakes. Cooper (2005) comparing the failure of dinosaurs to adapt to a changing environment, with a failure to adapt by those involved in intelligence, highlights the potential risks that are created by failing to evolve and develop methods:

> *Not unexpectedly, these routines "work" for the specific conditions they were developed to address. They rarely perform well for off-design conditions, however, and, often, the better they work for the design conditions, the more narrow the set of conditions for which they are appropriate. Paradoxically, the better they work, and, therefore, the more efficient the organization at its routine tasks, the greater the danger that the organization will fail to be sensitive to its environment and changes occurring there. As with the dinosaurs, scores of major American corporations have fallen victim to this pattern of "over adaptation" and "change blindness." The Intelligence Community runs the same risk.*

Furthermore, the reluctance of many involved to share intelligence with others brings about additional problems and needs further analysis. White (2004) commenting on this "obsession for secrecy" states:

> ...the reasons for not sharing intelligence crashed into the World Trade Center on September 11.

Notwithstanding these problems, there are two key challenges for all who are involved in intelligence work, or those that want to make a contribution to it. The first is to be clear about what intelligence is and to be clear about the role of those involved in it. Regardless if intelligence is contributing to law enforcement or the national security function, attempting to broaden the scope of those involved in collecting intelligence is a fundamentally flawed concept. It is akin to the notion that the police can cure all societies problems when in reality all they can do is manage the harm those problems cause. Broadening the scope of those involved in intelligence role will do nothing but divert their already limited resources and create unrealistic expectations about what the intelligence function can achieve. Furthermore, if one was off at cynical disposition one might argue that this broadening of intelligence role is an attempt by some to enter into a world from which they would otherwise be excluded and this brings us to the second challenge; namely the contribution that academia can make. Writing papers on intelligence does not make one an 'intelligence expert' even if such a thing existed. What those involved in intelligence work need is the expertise that exists in academia with regard research skills and knowledge, directed towards areas that will be of real practical use. There is a need for less the orising and much more of what Robson describes as 'real world' research (2011). Debating is good if one has the time to debate, but where lives are in danger action is needed. And even debating is wasted time when a subject has been talked to the grave. One can expend great energy philosophising and seeking to reinvent what already has been invented but a wheel is still and wheel and intelligence work is still intelligence work.

References

1. R. K., Betts, „Analysis, war and decision: Why intelligence failures are inevitable", *World Politics* 31(1), 1978, p. 61-89.

2. J. Buckley, *Managing Intelligence: A Guide for Law Enforcement Professionals*, (Boca Raton: CRC Press, 2013).

3. J. R. Cooper, *Curing Analytical Pathologies Pathways to Improved Intelligence Analysis*, 2005, available at: https://www.cia.gov/library/center-for-thestudy-of-intelligence/csi-publications/books-and-monographs/curinganalytic-pathologies-pathways-to-improved-intelligence-analysis-1/analytic_pathologies_report.pdf (accessed September 2012).

4. T. Fingar, „Reducing Uncertainty: Intelligence Analysis and National Security", (*Stanford Security Studies* July 20, 2011).

5. P. Gill, and Phythian, M. *Intelligence in an Insecure World*, (Cambridge: Polity Press, 2012).

6. D. H. Gray, and Slade, C. „Applying the intelligence cycle model to counterterrorism. Intelligence for homeland security" *European Journal of Scientific Research* 24(4), 2008, p. 498-519.

7. J. G. D. Grieve, „Ideas in police intelligence" in: Harfield, C., MacVean, A., Grieve, J. G. D and Philips, D. Eds. *The Handbook of Intelligent Policing: Consilience, Crime Control and Community Safety*, (Oxford: Oxford University Press, 2008), pp. 9-15.

8. M. Gross, *Ignorance and Surprise: Science, Society, and Ecological Design*, (Cambridge, MA: MIT Press, 2010).

9. C. Harfield and Harfield, K., *Intelligence: Investigation Community and Partnership*, (Oxford: Oxford University Press, 2008).

10. R. J. Heurer, „Psychology of Intelligence Analysis", (Washington, DC: Centre for Intelligence Study, 1999), available at: https://www.cia.gov/library/center-for-thestudy-of-intelligence/csi-publications/books-and-monographs/psychology-ofintelligence-analysis/PsychofIntelNew.pdf (accessed August 2012).

11. U. Hoffrage, and Pohl, R., *Hindsight Bias: A Special Issue of Memory*, (Champlain, NY: Psychology Press, 2003).

12. D. Innerarity, „Power and knowledge: The politics of the knowledge society", *European Journal of Social Theory, 16*(1), 2012, p. 3-16.

13. L. K. Johnson, *Handbook of Intelligence Studies*, (London and New York. Routledge, 2007).

14. S. Kent, „The Need for an Intelligence Literature". *Studies in Intelligence*. (Central Intelligence Agency Library, 1955). Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/2need.html (accessed August 2012).

15. M. M. Lowenthal, *Intelligence: From Secrets to Policy*. (Washington, DC: CQ Press, 2006).

16. D. McDowell, *Strategic Intelligence – A Handbook for Practitioners, Managers, and Users*. (Lantham, MD: Scarecrow Press Inc, 2009).

17. P. S. O'Hern, *The Intelligence Wars – Lessons from Bagdad*. (Amherst NY. Prometheus books, 2008).

18. M. Peterson, *Intelligence-Led Policing: The New Intelligence Architecture*. (Washington, DC: US Department of Justice, Bureau of Justice Assistance, 2005).

19. M. Phythian, (Ed), *Understanding the Intelligence Cycle*. (New York: Routledge, 2013).

20. J. Richards, *A Guide to National Security: Threats Responses and Strategies*. (Oxford University Press: Oxford, 2010a).

21. J. Richards, *The Art and Science of Intelligence Analysis*. (Oxford University Press: Oxford, 2010b).

22. C., Robson, *Real World Research*. (Chichester: John Wiley and Sons, 2011).

23. G. B., Rossman & Rallis, S. F., *Learning in the Field: An introduction to qualitative research* (2nd ed.). (Thousand Oaks, CA: Sage, 2003).

24. UK Government Home Office, *The National Intelligence Model: Providing a Model for Policing*. (London: Home Office, 2000).

25. M. A., Turner, *Why Secret Intelligence Fails*. (Potomac Books. Washington DC, 2006).

26. J. J. Wirtz, „The American approach to Intelligence studies”. In: Johnson L. K (Ed). *Handbook of Intelligence Studies* (London and New York: Routledge, 2007).

27. M. Warner, Sources and methods for the study of intelligence. In: Johnson L. K (Ed). *Handbook of Intelligence Studies*. (London and New York: Routledge, 2007).

28. M. Warner, „Wanted – A clear definition of intelligence.” In Aldrich, R. J. Andrew, C. and Wark, W. K. (Eds) *Secret Intelligence – A Reader* (Milton Park: Routledge, 2009).

29. J. White, *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security*, (Belmont, CA: Thomson/Wadsworth, 2004).

The Cyber Challenge for Intelligence

Julian RICHARDS[*]

Abstract

As the Information Revolution unfolds, it is becoming clear that the business of intelligence is facing a historically unprecedented level of challenge and transformation. This process entails not only fundamental changes to the way in which intelligence targets are behaving, but also to the way in which intelligence organisations themselves need to evolve to meet the demands of the new era. The Cyber Challenge, as we may characterize this process of transformation, entails a tremendous number of opportunities and risks for the intelligence business. In this paper, I present the nature of the challenge and the implications for twenty-first century intelligence gathering under a framework of four dimensions, comprising: the interplay between defensive and offensive operations; the question of how "cyber operations" should be defined; issues concerning ethics, legalities and authorisations in the new era; and intelligence workforce issues concerning skills and training. The paper concludes that, with a sound awareness of these issues and the right people in place, the intelligence business should be able to meet the challenge successfully.

Keywords: Information Revolution, cyber, Information Assurance, ethics, legalities, skills, training

Introduction

As security and intelligence follows society in moving resolutely into the Information Age, the question of how the cyber dimension should affect the business of intelligence starts to become more prescient. One could imagine that this process would follow a similar pathway to previous technological revolutions in history which had a wide-reaching effect on intelligence, such as the rise of radio communications, the telephone, and then the mobile revolution which took off from the 1980s onwards. In some ways, there is merit in viewing the present cyber revolution in similar ways. In other respects, however, I would argue that the transformation facing intelligence today is much more complex and much more difficult to navigate through than was the case with earlier revolutions.

In this paper, I examine the multiple dimensions through which the cyber revolution operates, when thinking about the ways in which it will affect the business of intelligence. To a large extent, this cyber revolution must be seen not only in ways in which it affects and changes the behaviour of intelligence target, but also in the way that

[*] Co-Director, Centre for Security and Intelligence Studies, University of Buckingham, UK

intelligence organisations are themselves structured and managed. The framework of dimensions of transformation I will present is structured around four factors. First is the manner in which cyber operations and activities encompass both defensive and offensive axes for the intelligence business. This feeds into the second dimension of transformational challenge, namely the question of what a "cyber operation" does and should constitute. The third factor involves a set of dimensions around the operations themselves, and specifically questions of law and ethics in cyber operations. Finally, I will argue that the cyber revolution will mean fundamental challenges and transformations for the nature of the intelligence workforce needed in the future, and the skills and training they will require to be able to operate as Information Age intelligence analysts. It is important to conclude from this analysis that, while the size and nature of the challenge for the intelligence business is large and arguably more complex than any previous transformational challenge it has faced, success is by no means impossible with the right planning and the right people.

Factor 1: defensive versus offensive

For many years now, intelligence organisations have recognised a close synergy between "Information Assurance" and active intelligence operations. The former has comprised many iterations. Initially, with the rise of computing power through the twentieth century, "Computer Security" was seen as a significant component. Now, we speak more generally about "Cyber Security" as more complex networks and systems supersede questions of individual computers.

Information Assurance (IA) is all of this and more. At root, IA is about two things. Firstly and most importantly, it is about ensuring that governments and their security forces can operate and communicate in secure ways, and are protected from hostile espionage and disruption by external forces. This usually includes a combination of monitoring changes in communications technology and ensuring that vulnerabilities and security best-practice are followed; and, in many (but not all) cases, having an official regulatory function over the agreement of encryption standards at national and international levels. The second element of IA, which again does not necessarily apply in every country, is for it to work in a symbiotic relationship with the intelligence gatherers. What we mean here is that the poachers and game-keepers work closely together.

The IA people know where the strengths and vulnerabilities of communications networks are to be found, and this information can be very useful for the intelligence-gatherers and can be used exploitatively by them in maximising their intelligence gains. Similarly, information flows the other way, in the sense that the intelligence gatherers will see vulnerabilities and exploitations of target networks as they monitor communications, and will be able to inform their own IA people lest they also fall prey to the same problems. As the Information Revolution has unfolded, the same questions have applied, but now concern a much wider and much more complex set of systems and networks.

What all of this means is that the defensive and offensive components of cyber intelligence are closely bound together. As indicated, this has always been the case to a certain extent, but the rise of complex cyber networks and the explosion in offensive cyber operations internationally means that the relationship between the two sides of the house have become much more complex and much more important. It is also the case that the speed at which new cyber exploits become apparent in global networks and the necessity to find almost instant protection against them before they can wreak havoc, has accelerated and become a massive challenge for the intelligence business. Malware such as Stuxnet, Flame and Duqu, and the damage they have the potential to cause, have generated a great deal of anxiety across the intelligence business.

Complex relationships in this new era are not just about the intelligence and IA sides of the organisation, however, but also about the manner in which IA must now be delivered by a combination of public and private actors. One of the features of cyber security is that it involves a complex and bewildering array of public and private stakeholders, some of whom do not necessarily make easy bedfellows. It is a matter of fact that much of what would now be described as critical national infrastructure (CNI), is not owned or managed by the government but by private corporations. This applies not only to civil communications networks but also to military systems in many cases. On the defensive front, this means that cyber security must be achieved with the collaboration of private companies, which can be complicated in terms of who pays for the measures to be put in place, and how far the state can mandate and regulate private corporations in doing so. It is a further complicating issue that many of the corporations involved are foreign companies, and, in some cases, may belong to potentially hostile countries such as China.

On the more active side of intelligence gathering (the offensive front), it is also the case that governments may wish to have access to data owned and operated by private network providers. The case of the UK's attempts to put in place a new Data Communications Bill mandating communications service providers to provide communications metadata to the government to assist the intelligence and investigation processes (an attempt which has so far failed in the face of political opposition); and some of Snowden's revelations concerning the US government's attempts to extract data from the likes of Google and Facebook, show that the public/private boundaries are very much blurred in the modern era, and carry with them no end of legal and operational complications. It is, nevertheless, a reality of doing intelligence in the information age and must increasingly be factored into the planning and management of intelligence operations.

Factor 2: defining cyber operations

These blurrings of boundaries between the defensive and offensive realms, and between the actors involved in the intelligence process, lead on to the question of how we define "cyber operations" within that process. Inevitably, activities in this area have grown up rather organically as new capabilities have arisen. In the spirit of target-centric intelligence operations, it is right and proper that deliberations should begin with the intelligence requirement and the appropriate gathering of information to support those requirements, rather than with the technologies and collection capabilities themselves. In this sense, being able to gather intelligence over the internet either actively or passively should be folded seamlessly into existing mechanisms such as Sigint and Humint collection. However, the process of integrating old and new intelligence-gathering mechanisms effectively, and ensuring that intelligence analysts understand and think creatively about the whole panoply of approaches available, are not necessarily immediately obvious and straightforward activities.

One of the initial questions is that of what cyber operations are intended to achieve, and this quickly reveals that they can cover a wide range of passive and active activities. At the passive end of the spectrum, the massive availability of readily-accessible data over the internet offers huge intelligence opportunities. This is the essence of Open Source Intelligence (Osint), and the need to integrate it fully into the intelligence process. As well as being a repository of information, however, the internet is also a mechanism through which people are communicating. Indeed, in many walks of life, it is becoming the dominant mode of communication in terms of messaging and social networking media. In some ways, the interception and gathering of this data muddies the traditional notion of Sigint, since “signals” are not really intercepted as such in an Internet context, but can merely be observed and read with the right connections to the net. At the same time, such technical issues should not really matter – it is all intelligence.

Unlike traditional forms of Sigint, cyber operations offer enormous new opportunities for more active operations. These can be characterised under the rubric of disrupt, shape, and destroy, although the latter category is controversial in the sense that there is much debate as to whether a cyber “act of war” (defined as causing physical death and destruction) has yet happened or is indeed possible.[1] Nevertheless, cyber operations offer a unique new opportunity to integrate passive intelligence collection with activities that might previously have been described as covert action, such as Distributed Denial of Service (DDoS) operations.

This is all well and good, but intelligence organisations are increasingly realising that the effect of such active operations cannot always be guaranteed or even recognised. Traditionally, covert action was undertaken sparingly and with a great deal of care. Now, if cyber operations are offering an opportunity for greatly expanded and enhanced active operations, the risks of unintended consequences (as well as the opportunity for intended ones) go up greatly. There is much talk in intelligence organisations about describing active cyber operations as “effects-based” operations. This applies both in the positive sense of achieving real-world effects through cyber activities, such as disrupting a terrorist or criminal group’s operations, for example; and to understanding the negative consequences that could flow from such operations, such as compromising a human source whose data connection to the internet had acted as a source of intelligence, or causing an ideological blow-back if covert active operations were uncovered.

These considerations further complicate the business of planning such operations. In many cases, such considerations are essentially about the ethics of intelligence (on which more below). In the physical example described above (namely the risk of inadvertently placing a human being in a dangerous position through compromising their data) such considerations are clearly identified. However, there are also more philosophical ethical considerations to be brought into the discussion, such as whether the internet should be a place for people to communicate freely and securely, without interference or manipulation by state security agencies. In a sense, this is the essence of the firestorm generated by Edward Snowden's revelations, and has attracted the ire of individuals such as the founder of the World Wide Web, Sir Tim Berners-Lee.[2] These are questions on a higher and more philosophical plane, not just for the intelligence agencies but for society at large.

On a more practical level of analysis, a recognition that cyber operations can encompass a wide spectrum of passive and active undertakings means that a wide range of actors can be involved. As with the blurring of the public/private boundaries described earlier in the context of information assurance and cyber security, cyber operations globally are today being conducted by a wide and sometimes confusing range of actors. Military personnel and civilian members of state intelligence and policing agencies are joined in the activity by state-sponsored or encouraged "hacktivists" or "netizens" (such as the APT1 group in China, or the Syrian Electronic Army)[3], and by self-motivated individuals working either alone or within loosely-formed associations (such as Lulzsec and Anonymous). Some of these actors are working cooperatively on state strategic goals, while others may be very actively working against them. Aside from being an important component in the difficulties of attribution of cyber attacks, this phenomenon can also have legal and ethical ramifications. For example, if a civilian in a state intelligence agency undertakes an active cyber operation that could be construed as an act of war under international law (such as causing the destructive failure of a piece of military equipment or element of critical national infrastructure), is the officer who pressed the button on the attack a "combatant" under traditional definitions, and, if identified, should they be subject to the Geneva Conventions, or to civil law? These questions might seem hypothetical at the time of discussion, but they could quickly become more pertinent, and intelligence agencies need to have thought them through if they are embarking on such cyber operations.

Factor 3: legalities, authorisations and ethics

As we move into a world of multi-faceted cyber operations, one of the key questions being asked is whether existing laws governing intelligence and security activity, most of which were drafted before the full impact of the information revolution had been envisaged, are still fit for purpose. There are two elements within this debate. The first concerns the issue mentioned earlier about whether the gathering of communications and other data from the internet can be seen as "interception of communications" as was traditionally understood in history. As described, the basis of traditional Sigint is that it intercepts signals moving from one part of the global network to another, and considers the nationality of both ends of the communications circuit and of the interlocutors in determining whether warranty is required for the intercept under national law. (These factors will vary between national legal regimes.) With the internet, however, two of these principles are greatly muddied if not eroded altogether. One is the question of whether communications on the internet are really "moving" from one place to another, or whether they are just there on a server somewhere to be picked up by whoever has access. The second problem is that of attribution and anonymity, which means that it is often very difficult to determine the identity, let alone the nationality, of any interlocutor on the internet. Unlike fixed telephone networks, users of internet-based communications services do not have to register their name and address, or where they do, there are no checks undertaken to determine whether the details are true and accurate.

What this means is that states conducting intelligence-gathering are at a greatly increased risk of inadvertently invading the privacy of many of their own nationals, and, as Snowden's revelations have shown, this can feed into disquiet among the public. The legal question is whether existing laws on intercept are still fit for purpose in the new environment. The answer to this question will, of course, depend on the specific legal instruments in place in any country.

The second area of legal complexity concerns more active cyber operations, and the problems in this area are particularly acute in diplomatic relations between countries. These are questions of international law, and specifically whether cyber operations need to be considered under the same sort of framework as international laws of armed conflict. There, the Geneva Conventions and other provisions ensure that signatories must at least attempt to obey some "rules of the road" in their conduct, and can be held to account by the international community if they do not. Many countries are now calling for similar provisions to be put in place at the international level around the use of cyber operations. For countries like the US, this may be becoming more attractive in the face of what appears to be unprecedented levels of cyber espionage emanating from a number of countries, with China accused of being very much at the top of the list. Curiously, however, both China and Russia are becoming more vocal about the desirability of such international agreements,[4] probably because they are worried about the enormous investment being made by other countries such as the US into cyber capabilities. For the US, meanwhile, the strategy is more complex than it initially seemed. While international agreements on limiting the use of force are clearly a good thing, measures which caused a compliant US to be disadvantaged against hostile actors who pay less attention to international treaties; and the curtailment of active capabilities which the US itself may wish to use, both mean that enhanced international regulation over cyber operations could be a double-edged sword.[5]

We have already mentioned some of the ethical issues emerging from cyber operations, and these are expanding at the time of writing to encompass ethical concerns about whether and how intelligence agencies should be involved in "big data" surveillance in the contemporary age. There is a subtle difference between law and ethics in this area. The law may allow certain operations to be undertaken – in some cases because such operations are new and the law has not yet had a chance to consider the environments in which they occur – but this does not necessarily mean that everyone agrees with the ethical or moral justification for such operations. Large Western intelligence agencies such as NSA and GCHQ have responded to the Snowden revelations vociferously to say that they have done nothing outside of the law, and take legal authorisation very seriously. But this has not calmed the public clamour about the ethical justifications for the intelligence agencies' operations. Clearly it is the case that the information revolution has proceeded much more quickly and widely than have developments in law governing surveillance operations, and intelligence agencies need to be very careful over how they proceed into these grey areas if they are to retain public trust. Part of that process will revolve around oversight mechanisms such as parliamentary scrutiny, and whether these are sufficient to ensure trust that the agencies are using these dangerous weapons carefully and appropriately. Again, how such oversight is structured will vary a great deal between countries, but every liberal democratic country should expect to have rigorous and accountable oversight of their intelligence agencies in place.

Factor 4: skills and training issues

The final factor in the transformational challenge for intelligence is that of the workforce within the intelligence organisation itself, and how it will be provisioned to deal with the opportunities and risks that will be thrown up by the move into cyber operations. Major shifts have occurred previously in history, both in the areas of technological development and of the geographical focus of threats, but it could be argued that the information revolution is of unprecedented scope and complexity in terms of the challenge for the intelligence business in reinventing itself.

As with any major workforce issue, the challenge covers a spectrum from the initial recruitment of staff, through their training, retention and long-term career development. For many organisations the challenges have been exacerbated by the particular generational aspect of the revolution: those who understand and use the new technologies are generally concentrated in the younger portion of the population, while the managers and policy-makers in the intelligence business are disproportionately peopled by those who were brought up in a world before the information revolution began (with some honourable exceptions). This is not necessarily an insurmountable problem, but is testimony to the speed with which the information revolution has unfolded.

The changes required are not just straightforward technical ones, or changes that will be easily solved by merely offering some new training courses. In many ways, the transformation is about a fundamental conceptual change about the way in which big data can be used defensively and offensively, and the ways in which it transforms not only intelligence opportunities but the very essence of the intelligence organisation's structure. The cyber revolution is not just a technical change, but also an intellectual one of extremely wide-reaching implications. A major part of the challenge is developing a "cyber mentality" among intelligence analysts and their managers, which is able to both spot opportunities for integrating cyber operations into the intelligence process; and to think clearly about the risks and consequences of such operations.

From the point of view of specific skillsets, however, the move into cyber operations means that a greater proportion of analysts with advanced computing and programming skills will increasingly be needed, to supplement the more traditional "generalist" analysts.

The recruitment, training and retention of such analysts is no easy task. For a start, much of the traditional recruitment of generalist university graduates is not necessarily aimed at more technically proficient analysts, and in many cases, new technically-oriented career tracks and training programmes need to be designed. Career pathways ideally need to offer a high degree of vertical advancement within the organisation while still allowing for conducting technical operations (rather than moving into general management, as is more traditionally the requirement with promotion within government). This is partly the reason for which the intelligence organisation does not necessarily easily attract and retain computing analysts whose skills are often highly marketable, and who can generally command greater salaries in the private sector. In countries such as Russia, there is evidence of a problem around drawing new “information troops”, as they have sometimes been called, from within the military structure, and particularly from conscripted troops: the sorts of people with good cyber skills are generally those best-placed to find creative ways of avoiding the draft![6] This is a very specific problem for countries with conscription, but it highlights the more widely-experienced mismatch between the needs of the intelligence organisations and the sorts of highly skilled civilian analysts who have the required skills.

The training required for cyber analysts is also an area in which contracting-out may make an increasing amount of sense, since the highly specialised technical training required may not be something that the intelligence organisation can deliver in-house in a cost-effective way. There are some signs that universities and other training providers are increasingly working with governments to deliver tailored cyber-security programmes.[7] Of course, at one end of the skillset spectrum are situated sensitive issues that could not easily be delivered outside of the intelligence organisation itself, but governments are increasingly realising that they can deal carefully with universities and other providers on more sensitive projects, if the right personnel and information security measures are in place. Generally, the cyber realm is becoming a critical area for “academic outreach” by intelligence organisations.

At the same time, there are clearly potential security risks with bringing individuals with highly advanced cyber security skills – and particularly those skills at the offensive end of the spectrum – within the inner sanctums of the intelligence organisation itself. In many cases, the sorts of personalities who are very advanced at hacking and manipulating complex and well-protected computer networks are often those with – at best - a highly ambivalent attitude towards state security.[8]This poses a real dilemma for the intelligence business: some of the hackers in the system are the sort of people who could be extremely useful for the government in achieving its cyber aims, but many of those people are the very last people the government would want to invite into its system. In many cases, the more advanced cyber analysts have a higher skillset than any other individual already working within the intelligence organisation, and thus could have the potential to cause untold damage within the system before anyone noticed. Again, this raises the question of whether intelligence organisations could effectively "franchise" some of their work to external bodies and actors, thus minimising the security threat. This is a high-risk strategy, however, and is rather similar to policing organisations' dilemmas in dealing with criminals to achieve their aims.

Conclusions

The rise of cyber operations within the intelligence business entails a complex and widely pervasive set of challenges and opportunities. As I have outlined in this paper, the transformation effected by the information revolution is not just about fundamental changes to the nature of intelligence threats and targets, and to the way in which they behave; but also to the way in which the intelligence organisation itself should be structured and staffed. Much of the required transformation is a deeply intellectual one. Intelligence organisations will increasingly need to "think cyber", not just in the intelligence-gathering opportunities presented by an effective and targeted cyber strategy that complements existing intelligence operations; but also in the defensive elements of protecting the organisation from hostile attack, and making sure the intelligence business is protected as best it can be while carrying out its operations. But thinking cyber also means considering the ethical and legal complications that are arising from the information revolution. In many cases, the march of technology has far outpaced the development of legislation, so all manner of cyber operations are not only attractive for the intelligence organisation, but operate in something of a legal vacuum. The fact that something is legally authorised (or, at least, not explicitly ruled out by existing legislation) does not, of course, mean it is the ethical or right thing to do. This is the essence of the furore unleashed by Edward Snowden's revelations about the scale and complexity of data gathering operations undertaken by the likes of NSA and GCHQ. If the public are to retain trust in their intelligence organisations, then the latter must think about these legal and ethical issues as carefully as they think about the intelligence opportunities presented by the cyber revolution.

References

[1] See, for example, Thomas Rid's comprehensive critique of the notion of cyber war: Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst and Co, 2013)

[2] See The Guardian (19 December 2013), "Tim Berners-Lee leads call for more transparency over mass surveillance". http://www.theguardian.com/technology/2013/dec/19/tim-berners-lee-data-privacy-surveillance accessed 4 February 2014

[3] See Julian Richards, *Cyber-War: The Anatomy of the Global Security Threat*(Basingstoke: Palgrave Macmillan, 2014), pp.33, 48

[4] See TimMaurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities of the UN regarding Cyber-Security". Cambridge MA: BelferCenter for Science and International Affairs, September 2011

[5] Julian Richards, *Cyber-War: The Anatomy of the Global Security Threat* (Basingstoke: Palgrave Macmillan, 2014), p.8

[6] Keir Giles, "Information Troops – a Russian Cyber Command?", in C. Czosseck, E. Tyugu and T. Wingfield, (eds.) *Proceedings of the 3rd International Conference on Cyber Conflict* (Tallinn: CCD COE, 2011), p.54

[7] See for example the postgraduate cyber security programme at De Montfort University in the UK: http://www.dmu.ac.uk/study/courses/postgraduate-courses/cyber-security.aspx

[8] Note, for example, the case of the hacking group "Lulzsec", which was interdicted and broken-up by the authorities in 2011 after one its members turned informant for the FBI: Parmy Olson, "We are legion, expect us." *The Sunday Times Magazine* (4 August 2013), pp.14-19

Targeting Memory Processes Can Be a Useful Tool in Counter-Terrorist Strategies

Cosmin-Dragoş DUGAN[*]

Abstract

After 12 years of war against global terrorism, the threat becomes less intense but more sophisticated and pervasive.

Today's new generation of terrorists constitutes the third wave of radicals stirred to battle by ideology.

Using a neurobiological approach, we take into discussion the causal factors, neuro-physiological, psychological and genetic/ epigenetic mechanisms involved in violent radicalization and aggressive behavior. We also analyze the possible connections between non-political vulnerable groups that are misusing Internet (internet addicted, violent MMORPG's and FPS's addicted players, suicidal individuals, etc.) and the risk of online radicalization and recruiting. A special attention was paid to online radicalization (cyber-radicalization) and to the Internet as a tool used by terrorists for intensifying and accelerating recruiting.

In this paper, we want to emphasize that using various techniques that are targeting cognition, especially memory and learning – such as distortion techniques (retrieval-induced forgetting, disrupting memory reconsolidation, post-event misinformation, false recognition, motivated forgetting), cognitive dissonance (subliminal conditioning and perception) or even the manipulation of epigenetic mechanisms – can be a useful tool in countering violent extremist narratives, especially by interfering with the "identity-building" process. If successful, these methods will help promote a tailored counter-narrative and will facilitate counter-radicalization efforts as well as the detection of concealed information.

If in the next decade the Internet will continue to evolve and reshape our lives, so is the knowledge about our mind. At the end of our paper we discuss several research trends in neuroscience and cyber-psychology that can provide useful tools for online counter- and de-radicalization.

Keywords: memory bias, forgetting, deception, counter-narrative

Introduction

After more than a decade in the 21th century, it appears that global terrorism is far from becoming predictable and controllable over long periods of time; in fact it is rather seen by some analysts as one of the driving forces that pushes global politics in a post-Wesphalian era[1]. Fragmented over large geographical areas

[*] MD, „Elias" Clinical Emergency Hospital, Romania

but not defeated, terrorist organizations are evolving, carving new survival strategies and waiting for future opportunities to strike again. Large and complex organizations have been dismantled, favoring the development of smaller but harder to detect terrorist entities. Blended in multiethnic tolerant Western societies, apparently “good citizens” but with the mind saturated with “ideological fuel”, can become real soldiers in this unconventional warfare. Unable to attack significant symbolic objectives or provoke mass casualties, they become “dealers of fear”, being increasingly less discriminative when choosing targets and violent methods while learning to make good use of social - and mass-media. Social and economic disruption, and especially the development of persistent fear and feelings of insecurity are essential in achieving the political ambitions of terrorist organizations and in undermining the trust of the citizens in governmental authorities. Major terrorist incidents inflicted significant psychological traumas in a largely unprepared population, but also triggered social defense mechanisms that increased resilience and societal cohesion. As a result, a broad spectrum of specialists from virtually all the scientific (and even artistic) branches identify terrorism as a major societal threat and become interested in developing new and innovative strategies that will eventually lead to the extinction of this hazard.

The medical profession is involved in many aspects concerning terrorism and the rapid development of various areas of research in the last years produced practical knowledge that can help the national security community. The result is a proliferation of cross-disciplinary approaches in many subfields of international relations and security, including terrorism studies. In particular, the speed, sophistication and dual-use capabilities of new developments in neuroscience and neurotechnology have contributed to the identification of interactive areas that could affect and be important for national security[2]. For example, a review of the publication rate of science articles since the September 11th attacks focused on keywords that included terror or national security and words like brain research or mind reading has shown a considerable increase to 147 articles in recognized science journals within the period 2001 to 2011 as compared to 25 articles between 1991 to 2001[3]. Hot topics include the use of neuroimaging techniques, brain stimulation techniques, neuropharmacological agents, neural interface systems, neural enhancement, neuroergonomy, protection from neurotoxins, social neuroscience, detection of concealed information, etc.[4]

Following this trend, we review the scientific papers of the last decades searching for synergies between various studies involving human cognition (especially studies on human memory) and terrorism related risks. As a result selected applications will be presented in this paper, regarding two main scenarios: reducing the psychological trauma induced by terrorist incidents via altering traumatic memories and preventing cyber-radicalization using various memory distortion techniques.

Coping with psychological trauma induced by terrorism: altering traumatic memories

The broad goals of terrorism are ultimately psychological, trying to affect the entire population well beyond the scope of physical destruction by making ordinary people feel vulnerable, anxious, confused, uncertain and helpless. This is why the long-term effects of terrorism on brain, behavior and physical health must be understood in order to be able to predict the most affected social groups and elaborate interventions that might promote resilience at individual and population level[5]. While the intensity of the initial emotional trauma is related to some quantifiable factors, such as physical and psychological/mental distance between the subject and terrorist incidents, personal physical injuries, material loses, etc, over time - media overexposure, specific language (emotional, metaphorical and historical) and angling (developing patterns of association) are increasing the prevalence of severe lasting psychological effects.

Post-traumatic stress disorder (PTSD) is the most common type of psychopathology experienced in the aftermath of large-scale traumatic events[6]. The disorder involves substantial functional impairment (recurring flashbacks, avoidance or numbing of memories of the event, hyperarousal) long time after the exposure to the traumatic event and is often comorbid with other mental health conditions such as depression, generalized anxiety disorder, and substance abuse[7]. Decades of studies confirmed the correlation between terror attacks and widespread PTSD symptoms in the targeted population[8,9,10]. For example, an early study of post-traumatic stress disorder (PTSD) among 9/11 survivors indicated that up to 20% of residents living close to the World Trade Center had suffered acute symptoms of PTSD, with elevated levels of depression throughout New York City[11]. But while some PTSD symptoms are considered "reasonable" up to a certain degree for short periods of time after a terror attack, long-term symptoms are considered pathological and need specialized intervention.

Powerful emotions stirred by terrorist incidents instigate various mechanisms, both in normal individuals as well as in those with PTSD symptoms, that have seriously disruptive effects on the encoding and integration of the traumatic event in memory. Above all, different types of intrusive memories are responsible for the persistence of PTSD symptoms and behavioral changes. For example, patients report a high frequency of involuntarily triggered intrusive memories involving reexperiencing aspects of the event in a very vivid and emotional way but their intentional recall is fragmented and poorly organized, with missing details and difficulties in recalling the exact temporal order of the events[12]. Some "benign" form of autobiographical memories called "flashbulb memories"[13] seem to be ubiquitous in the case of 9/11 events, having been reported by individuals regardless the age[14,15,16] all over the world, not only by New York City residents. On the other hand, flashbacks[17], were less frequent and reported mainly by vulnerable individuals but they were more often associated with the development of PTSD or other forms of anxiety disorder. Multiple studies in the last decades proved that long-term retention of traumatic memories associated with terrorist incidents facilitate the development of psychiatric disorders, which can be very debilitating and seriously affect a person's quality of life.

Extensive research showed that psychological sequelae and especially PTSD are responsible for significant behavioral changes. Consumption of tobacco, alcohol and marijuana increased in the first 6 months in the population located near major terrorist incidents sites such as Manhattan or Oklahoma City[18] but it was not identified in remote locations[19]. Driving behavior is also affected in the first week after a terror attack, studies (in Israel and the US) showing a significant increase in light and fatal car accidents (by almost 30%)[20,21]. Disturbances of instinctual behaviors are frequent in the first three months, such as eating disorders, sleep disturbances[22,23] and sexual behavior changes[24,25]. The dreaming experience after traumatic events is of particular interest because it can help understand how different aspects of personality relate to pathology and how the subconscious mind communicates with the conscious brain. Systematic research regarding the impact of 9/11 on dreaming showed that the attacks had a tangible impact on dream content, but it did not fundamentally alter the dreaming process[26]. The main, and highly significant change was an increase after 9/11 in the intensity or power of the central imagery of the dream[27]. Interestingly enough, one study discovered that for each hour of TV viewing (but more a three hours) in the first day of the 9/11 incident there was a statistically significant six percent increase in the proportion of the dreams containing a specific reference to the attacks[28]. However, the levels of suicide mortality have not changed, which goes to show that extreme responses are uncommon after a terrorist attack[29].

Chronic PTSD induced by terrorist incidents is also responsible for functional and structural brain anomalies. PTSD is frequent accompanied by other types of mild cognitive impairment such as lack of attention and concentration, poor working memory[30] and slow learning of novel word associations[31]. Converging evidence from neuroimaging research suggests that this altered information processing is associated with differential functional neuroanatomical activity in PTSD, such as volume decrement of grey matter in anterior cingulate cortex[32,33], smaller hippocampal volume[34], smaller left amygdala and in other structures from frontal lobe and limbic system[35]. Neuroendocrine disorders such as autonomic reactivity and hypothalamic pituitary adrenal axis dysregulation are also frequent[36] and they are accompanied by modification of the gene expression pattern involved in glucocorticoid receptor regulation, signal transduction, brain and immune cell function[37].

Another stunning feature in the case of survivors of terror attack with chronic PTSD is the increased psychiatric risk for their offspring, due to possible independent transgenerational epigenetic inheritance. Epigenetic alterations were described in PTSD cases, explaining the long-lasting effects after exposure to traumatic stimuli[38]. In particular, they involve mechanisms associated with fear memory consolidation and reconsolidation, fear memory extinction and fear conditioning[39]. Transgenerational inheritance of stress response, when not only the mother (especially during pregnancy)[40] but also the father[41] has been exposed to a stressful environment, can extend across multiple generations. A few studies were conducted in the case of PTSD induced by terrorist incidents, but they support the idea of intergenerational transmission[42]. Transmission via epigenetic mechanisms of stressful visual memories (flashbacks) from an exposed mother to a offspring, mentioned by some researchers in psychogenealogy[43], was not described, but it is still a matter of debate[44].

The societal and economic burden induced by long-lasting psychological effects caused by terrorism are difficult to measure, because they are sometimes "hidden" from official statistics but they are imprinting the individual and collective behavior. The broad spectrum of psychological reactions after a terror attack impose the necessity of a customized approach, which includes, among other measures, the management of traumatic emotional memories. Three main strategies are discussed hereafter: resilience (psychological immunization against trauma), recording personal thoughts and emotions and altering traumatic memories.

Resilience strategies are preparing individuals and communities to adapt themselves to the challenge by retaining flexibility, adaptability, functionality and empathy. Case-studies, mock-up exercises, survival training and the understanding of mechanisms of the group and social-cohesion can prove invaluable when confronted with powerful distress caused by terror attacks, leading to enhanced coping and positive expectations. Sharing positive information while suppressing rumors and fear from spreading across the general population prevents psychological contagion. Evoking collective and positive memories about historical figures or events can restore a sense of confidence. Prior identification and classification of the individuals and societal groups that are more vulnerable to trauma exposure enable early interventions in critical cases[45].

Recording personal thoughts and feelings soon after a massive terrorist attack proved to be invaluable for socio-psychological studies. Even if the memories are usually complex and rich in details, due to the tense social environment and media overload they are vulnerable to different forms of manipulation or forgetting. Recorded memories have a higher degree of confidence then those recollected after a period of time, helping us to understand how people reconstruct the past before a dominant public narrative has been created by those who have a vested interest in defining the political meaning of events. For example, in the case of the 9/11 incident the official account portrayed a nation unified in grief; it also allowed government officials to claim that there is a public consensus that the terrorist attack was a turning point in the nation's history with significant implications for national and foreign policy. But this interpretation was not constructed by the victims of the attack but by those who had observed it and had political reasons to interpret it as they did[46]. In such cases, the memory becomes a prisoner of political reductionism and functionalism, being transformed in a "corollary" of political development and interests. In the effort to understand how individual and social memory is constructed, many universities or NGOs started immediately after the 9/11 and other terrorist-related incidents to carry out surveys and opinion rolls to asses the cognitive and emotional impact of the events on the nation's psyche. More then a decade later the results are still cited and used in scientific papers, providing a detailed and extensive framework.

Traumatic memories can become a dramatic burden, altering the life and even the identity of the victims of aggressions and sometimes those of the families and close relatives[47,48]. Patients with chronic PTSD induced by terrorist incidents or with prior psychiatric disorders become unable to prevent the recall of intrusive memories of negative autobiographical events and as a consequence, significant disruption of day to day life follows. Extensive medical guidelines are recommending various procedures that alleviate major symptoms of PTSD mainly by interfering with the physiological, psychological and socio-cultural mechanisms that influence memory formation and recall[49]. Early psychological intervention (for example, primary intervention for memory structuring and meaning acquisition – PIMSMA) offers a prompt structuring of traumatic memories as soon as possible after formation, before they can be consolidated. Unfortunately, this kind of approach has a limited effect in reducing the subsequent rates of posttraumatic stress syndrome in survivors of terrorist attacks but is being effective as a form of supportive care[50]. Moreover, survivors who develop partial or chronic PTSD will require complex therapeutic measures – psychotherapies (cognitive therapy, exposure therapy, and eye movement desensitization and reprocessing) and pharmacotherapy (sedatives, mood stabilizers, antidepressants, antipsychotics)[51]. Radical therapies as electroconvulsive therapy or cranial electrotherapy stimulation, that can be followed by retrograde autobiographical amnesia, are taken into consideration only in exceptional cases[52].

But even if therapeutic forgetting promises a better life for traumatized victims and true memory erasure is still the domain of dystopian science fiction genre, ethical and legal issues still remain to be discussed in democratic societies. Memory-dampening drugs can affect not only the emotional aspect but also the informational content of traumatic memories leading to a conflict between the individual interests of the having a better control over his memories and society's interest in preserving evidence that benefits others[53]. In other cases, during psychotherapy false details are deliberately planted into a traumatic memory, without the knowledge of the patient, who will become an unreliable eyewitness. Translating ethical obligations to remember into legal restrictions on memory dampening is not easy and must be balanced. Ethical concerns regarding the process of memory erasure are underlining that it may damage the psychological well-being by degrading or dehumanizing the quality of life[54]. Other concerns are pointing to the close link between memory and identity. While memory is not the sole constituent of personal identity, it creates much of the psychological continuity that makes us aware of our continuing existence over time. So, the process of memory dampening may weaken or distort our sense of identity by dissociating memories of our lives from those lives as they were actually lived[55]. As a result, reaction to horror and tragedy could be blunted, allowing stressful events to be encoded as neutral emotional experiences. But this in not a new process, argue cognitive libertarians, because we constantly construct ourselves from memories that are largely inaccurate, biased, or even false; so it is arguable that modifying a few memories can radically change our narrative identities.[56]

When available, neuroepigenetic reprogramming will interfere with the readout of memory-related genes changing the biochemical underpinnings of memory storage and maintenance[57]. Altering the process of transgenerational epigenetic inheritance can also short-circuit beneficial evolutionary pathways, poorly understood at the moment and difficult to predict over many generations[58]. Opponents of this vision argue that memory dampening via pharmaceutically-assisted rewriting may strengthen the sense of identity by allowing an alternative and selective reconstruction of our lives[59].

In conclusion, terrorism victims must be screened for PTSD or other anxiety disorder symptoms for long periods of time after the initial exposure in order to enable early interventions in critical cases. As terrorism is a psychological weapon, evaluation of the distribution and degree of emotional trauma following an terror attack should include complex studies on cognitive abilities, including memory and learning. Understanding how individual and social memory is constructed in stressful situations allows the identification of the dominant memes, their characteristics, malleability to manipulation and the general pattern of transmission. As a last resort, alteration of individual and collective memories, using a broad spectrum of methods (psychological, medical, socio-cultural) should be taken into consideration in order to obstruct terrorist organization from spreading fear and interfering with political decisions.

Preventing online radicalization using memory distortion techniques

After 9/11 an increasing number of individuals and groups advocating violent online political extremism and in particular violent jihad have significantly strengthened their online presence. Internet became a tool used for spreading propaganda, attack planning and preparation and even online radicalization. Its popularity among terrorists lay on the fact that it had dramatically reduced the cost of communication while facilitating interpersonal interaction and network formation. With the establishment of

„deterritorialised" virtual networks of believers and the ability to partially replace traditional physical gathering spaces used for recruiting, like mosques, community centers and coffee shops, Internet became a real radicalization accelerant. Rapid changes in the Internet landscape, due to technological sophistication and increased access (dark web, deep web) provided a myriad of possibilities for violent and extremist organization to boost their online presence. For example, mobile Internet is increasingly popular among youths, while social-media is offering free access to social networking, video sharing, blogging or micro-blogging sites[60]. While highly-organized, hierarchical groups prefer centralized websites and diffusely-structured networks to distribute their content to third-party distribution entities, smaller groups or even (super-empowered) individuals make use of an array of decentralized, mostly-unofficial, privately-owned web pages, blogs, web forums and online bulletin boards[61]. "Virtual media production and distribution entities" (MPDEs) are offering their assistance to disseminate and enrich the online content (photos, videos, statements or religious doctrines) of diffuse jihadist groups. The use of Internet for spreading ideology as opposed to the traditional oral and written transmission also has the incontestable advantage of digital information that can be stored, mined, combined, collated, shared, reused, modified and remixed. New memory technologies can make some form of forgetting impossible or at least uncertain, in a time when accumulation is easier than sorting and selecting, deletion is less common than accretion[62].

Theoretical approaches to different aspects of recruitment and violent radicalization and decade's worth of experience place ideology and means of propaganda at the heart of the terrorist phenomenon. Even if the methods and the ideological roots can be traced back into history, the rapid change of the social and technical environment demands that old theories be revised and in some cases even reconceptualized generation after generation. A hallmark of the terrorist organizations after 9/11 is the increasing use of online radicalization via global virtual networks. Virtual social networking allows people to stay in contact with like-minded individuals and engage themselves in low risk/low cost forms of political activism.

With time, some members will become more and more involved in group activities and part of belief networks, communities that share powerful emotional ties constructed through repeated exposure to narratives and ideology. The importance of narratives in the process of recruiting and radicalization is based on solid observational correlations between long-term online exposure and gradual changes in motivation, perception of reality and behavior[63,64].

A narrative "is a system of stories that share themes, forms, archetypes and myths. Every story in a narrative need not have exactly the same characteristics; however, they relate to another in a way that creates a unified whole that is greater than the sum of its parts"[65]. Narratives can alter a person's beliefs, attitudes and intentions, may consolidate memory, cue heuristics and biases in judgment or influence group distinctions, framing the world in which an individual lives while providing an alternate form of rationality that may lead a person to yield to persuasive calls to action[66]. The use of storytelling and narratives as powerful cohesive elements of cultural identity allows the discrete insertions of ideological memes as part of a narrative rationality disguise under an acceptable and apparently inoffensive cultural skin. The effectiveness of online narratives in the process of "identity-building" and radicalization created the necessity to find alternative ways to invert the role and identify effective means to counter-violent extremist narratives in an attempt to facilitate the counter-radicalization and de-radicalization efforts[67]. Building, conveying and publicizing a comprehensive counter-narrative requires the ability to cover the major dimensions of the violent extremist ontology in question (political, historical, socio-psychological, theological, instrumental), making use of sophisticated ideological counterarguments and being supported by credible messengers[68]. For example, offering alternative models and ways to heroism, adventure, a transcendental sense of one's purpose and meaning in life may prove more effective in diverting quixotic but heartfelt youthful commitment to less violent paths[69].

"Winning the minds and souls" of extremists using tailored multi-layered counter-narratives requires the fusion and an in-depth knowledge of ethnography, anthropology, sociology, neurobiology, computer science and mastery of narrow interdisciplinary domains as psycholinguistic, memetic engineering, neuroepigenetics, neuroeconomy, parapsychology etc. One of the most interesting and sophisticated initiative is DARPSA's "Narrative Networks", dedicated to the understanding of how narratives influence human cognition and behavior, and applying those findings in international security contexts[70]. Central to this program is the study of the neuropsychology of narrative (impact on hormones and neurotransmitters like serotonin and oxytocine, reward processing, emotion- cognition interaction) and its effects on persuasion and the development of models and simulations of narrative influence in social and environmental contexts[71]. The main outcome of this project is the creation of software and hardware capable of detecting narrative influence and predicting responses, enabling prevention of negative behavioral outcomes as a result of narrative actions and capturing the transition from changes to beliefs, desires, attitudes and finally to actions. Other programs developed by IARPA are designed to recognize and use metaphors in complex cultural narrative contexts in order to influence beliefs and attitudes[72] or to understand sense-making and the role of cognitive biases related to attention, memory, and decision making[73]. Similar software for civilian applications are used as meta-journalistic platforms, being able to analyze specific data sets and transform them in narrative content easy to read and comprehend[74].

Due to a strong connection between memory and personal identity[75], cultural memories and group identity, we emphasize that studies on human memory and in particular on malleability and forgetting can be useful in designing successful counter-narratives against violent and extremist organizations. Memories are potent sources of motivated behavior and numerous experiments showed that behavioral alteration can be induced by selective forgetting or memory distortions. Some of the memory biases that are potentially useful in making counter-narratives are mentioned hereinafter.

Building a memory involves a constructive and reconstructive process that can be altered by expectations before events ever happen or by rumination after the event took place. First of all, false memories arise from the same encoding processes that produce true memories; in this way we may never know with absolute certitude that a specific memory is an unbiased representation of a true event. Neurobiological researche confirmed that several adaptive cognitive processes (such as simulation of future events, semantic and contextual encoding, creativity, and memory updating) that contribute to the efficient functioning of memory, are prone to distortions as a consequence[76].

Classical methods of propaganda act before the target is exposed to new information, manipulate individual perception or alter the content of the news, interventions that in a globalized world may not be always possible or have a negligible effect. For this reason, the manipulation of preexisting memories of real events becomes crucial in the efforts to change the collective memories in a social network. The most accessible method is by using the post-event misinformation paradigm witch employs the providing of erroneous information following the initial encoding. The altered memories obtained using this method are resilient, fMRI studies revealing that many of the same brain regions that support encoding of true memories also support the encoding and incorporation of incorrect information, leading to subsequent false memories[77]. Other useful memory biases are gist-based and associative memory errors, when people falsely recall or recognize an item that is perceptually or conceptually related to an item that they did encounter previously, but they fail to recollect specific details of an experience and instead remember just the general information or the gist of what happened. A different type of memory distortion that can be used in order to create false memories is imagination inflation which, is based on the fact that when we are imagining a novel event, we tend to miscombine elements of memory and imagination[78]. Neuroimaging studies are supporting the constructive episodic simulation hypothesis showing that imagining possible future events and remembering past events recruit the same „core network‟, which consists of the medial prefrontal and medial parietal regions[79].

Retrieval-induced forgetting (RIF), a more specific and complex effect, is produced when using the retrieval of a preexisting memory as a way to induce selective forgetting for the unmentioned but related memories rather than the unmentioned but unrelated memories.

This is probably because when people attempt to retrieve a specific memory (discussing about past events[80]), related memories compete for activation and to ensure that the desired memory comes to mind, the competing memories must be inhibited. This inhibition can linger over time, but can be augmented by ample retrieval time, facilitation and effective long-term retention[81]. Also, the memory of an event can be experimentally dissociated from the belief in the event's occurrence; for example, after the creation of powerful false memories, debriefing can leave behind vivid false memories which are no longer believed, proving that belief in and memory of an event can be independently-occurring constructs[82]. RIF is relevant to the effects of social interaction on memory because it can occur not only for a speaker in a conversation (within-individual retrieval-induced forgetting WI-RIF), but also for listeners (socially shared retrieval induced forgetting (SS-RIF).

SS-RIF arise because listeners concurrently but covertly remember along with speakers (with whom they share an identical or similar past) and they should manifest the same pattern of induced forgetting as the speakers[83]. The context is also important, especially on the way the listener monitors the speaker; apparently SS-RIF emerges when listeners monitor for accuracy but not for the fluidity of the speaker's response. In this way, even moments of silence that may appear in an act of conversational remembering produce similar patterns of induced forgetting in both speaker and listener[84]. Another particularity is that SS-RIF is gender-sensitive, being observed only if the participants are of the same sex[85]. Recent experiments showed that SS-RIF can be found for a wide variety of material, including schema relevant and irrelevant information, autobiographical memories, emotional and highly rehearsed memories. Socially shared retrieval induced forgetting was found not only to shape an individual's own self-construal, as well as the self-construals they share with others but also it increases the social connection among discussants[86].

This cluster of effects is an ideal tool when wanting to socially reshape the past in the process of collaborative remembering (transactive memory and collaborative facilitation) and probably influence future social behavior[87]. For example, experiments in which was probed the participants' memory of the September 11 terrorist attacks showed that SS-RIF is a robust effect and it can be used for the "sanitization" of the listener's memories[88]. Another useful application is in the removal of sensitive or offensive collective memories shared by individuals from virtual social networks and the manipulation of target behaviors. In this case, the relation between the characteristics of the social network and the capacity to transmit and store memories is influencing the spread of forgetting and the efficiency of consensus building. For example, one type of network could allow the quick transmission of a memory across a social web but not necessarily promote convergence, whereas another network might promote rapid convergence once transmission is complete but make network-wide transmission difficult. Even if convergence does occur, a collective memory will emerge if shared individual memories remain stable over time[89]. More research is needed in order to establish how the changes of configuration of the social network alter the collective memories and the process of sharing.

Music is another item that has the potential to influence attitudes, social norms or behaviors to such an extent that it can intensify or diminish the trajectory of intergroup conflict, especially among adolescents who are more susceptible to peer pressure[90]. Music is of particular interest when designing a tailored counter-narrative because it is largely used by a growing number of extremist organizations in propaganda materials. For example, two distinctive musical genres are the primary vehicles of radicalization music: hip hop and Nasheeds (chant-like forms of music without instrumentation). Islamic hip-hop, considered to be a subgenre for religious education and identification, was utilized by Al-Shabaab (Abu Mansoor al-Amriki), Arab League and Soldiers of Allah, with the purpose of promoting social change through armed insurgency[91].

First of all, music can be used for countervailing messages that admonish violence and intolerance; critical to success is the emotional content, the role played by the performer in framing the context and message, the broadcast medium, and the use of messaging and themes to link emotions with musical and lyrical content[92]. Another area of intervention is to use music and musical preferences as a basis for furthering intergroup dialogue and as a way of reducing intergroup conflict. The synergies between music, selected lyrics and language perception is essential, as underlined by studies of psycholinguistic and neuroimaging. Under the shared syntactic integration resource hypothesis (SSIRH), music and language draw on a common pool of limited processing resources for integrating incoming elements into syntactic structures, a functional link that is confirmed by recent neuroimaging studies that are revealing a partial overlapping between neural correlates of musical and linguistic syntactic processing[93,94]. Even more challenging, mood induced by music is also reflected in visual awareness, both in biasing processing sensory input, and in the generation of conscious visual percepts in absence of structured visual input[95].

Deceptive speech can be used in conjunction with selected musical parts in order to increase the cognitive and emotional dissonance in a counter-narrative message. Researches in this domain focused on the changes in the speech signal when people were being deceptive and the relevance of speech cues in detecting deception. Due to the fact that deceptive speech is individualized and very multifaceted, new parameters such as speaking and articulation rate, duration and frequency of filled and unfilled pauses, diphthong trajectories and consonant articulation are studied[96].

Visual content, such as photos or suggestive drawings can furnish the imagination with content resembling percepts, thereby fostering false memories, effect which is amplified when the photos are in color. This, is particularly important because television, mass-media and social-media are often the primary channel through which we learn about public events of the past and the present, and they are generally trusted as reliable sources. Even if the capacity of producing false memories using altered imagery of global events is weaker then in the case of narratives[97] in some conditions the effect can be attained very quickly, in only 4 to 12 seconds[98,99]. More importantly, exposure to a doctored photograph is influencing not only people's memory for a past event, but also their attitudes and behavioral intentions (for example they might help people manufacture thoughts and images about other claims such as belief or feelings of truth)[100]. The most common form of manipulation using visual content is by surrounding false photos with a large number of true photos as part of a combined narrative representative for an iconic public event. A similar effect of distortion of old and recent autobiographical beliefs and memories was obtained using doctored videos[101]. Interestingly enough, the use of functional magnetic resonance imaging in studies about the neural substrates of memory errors showed that false recognition is not a unitary phenomenon, but rather can reflect the operation of two distinct cognitive and neural processes. In the case of visual stimuli, a particular relationship between unrelated false recognition and language-processing–related activities was noted, sustaining the hypothesis that unrelated false recognition for novel visual information reflects a verbal matching strategy[102]. The importance of this process was recently tested, showing that when information associated with verbal labels matches stimulus-driven activity, language can provide a boost to perception, propelling an otherwise invisible image into awareness[103]. This effect can be used for the development of memory biases using language-specific perceptual processing of visual images. Another factor that influences the success rate of robust memory formation is the web site architecture. Neuromarketing studies showed that while a lineary structured web has a superior impact on consumers memory, an interactive structure will have a superior impact on consumers attitude toward the content of the site. The optimum reaction towards the site's content is obtained through a compromise formula, exposing the viewer first to a linear structure and then to a interactive structure[104].

In future, the development of emerging scientific fields (such as quantum- and super-computing, neuroscience, nanotechnologies, advanced genetics) will help envision innovative tools for advanced neuro-cognitive warfare. Soon computers that mimic the brain's activity will be able to pass the Turing test and mimic some of the most “human” traits – the ability to deceive while detecting the lies of other humans[105]. Advances in neuroergonomy and nanotechnology will allow brain-to-brain or brain-to-machine communication, making transhumanism more plausible. “Knowledge accelerators” similar to FuturICT will be able to run complex deep analysis and large-scale simulations of global events browsing the whole Internet in near-real time allowing for more accurate early-warnings[106].

In the end, neuroscience will enrich the knowledge about mind and society, with our consent or without it, but the ethical and legal boundaries that protect our rights to privacy may be the price to pay.

Conclusions

Ideology and propaganda are key factors in the process of recruitment and radicalization, being responsible for the expansion and continuity of the terrorist phenomenon. Countering terrorist organizations by means of neocortical warfare, which employ the “weaponization” of psychology, anthropology, neuroscience etc. should lead to major breakthroughs in the “mind wars” that precede and cause the terrible actions designed to inspire fear at a large scale. Even if this approach is considered a “soft strategy” on short-term, history taught us that the use of force is ineffective on erasing cultural memeplexes; on the contrary, they thrive under oppression, becoming more resilient, finding new ways to spread using vectors and hosts and optimizing their life cycle. In the XXth century, the defeat of devious political systems based on utopian and hate-ideologies was achieved when citizens refused to believe and became immune to propaganda. In a world dominated by technological and scientific revolutions, global markets and freedom of thought, it's just a matter of time until individuals infected with the most aggressive ideologies have possession, and most likely use, the most destructive weapons. Targeting the ideological roots of extremism and limiting the spread of vicious propaganda will eventually lead to loss of political momentum and legitimacy of terrorist organizations. As a psychological weapon, terrorism must be defeated in the same environment in which it was born: the human mind.

References

[1] Robert A. Manning, “US Strategy for a Post-Western World”, Atlantic Council of the United States, 2012, pp. 6, Washington, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=156307

[2] Chris Forsythe, James Giordano, ”On the need for neurotechnology in the national intelligence and defense agenda: Scope and trajectory”, *Synesis: A Journal of Science, Technology, Ethics, and Policy*, No. 2, 2011, pp. 5-8 accessed 29 August 2013, http://www.synesisjournal.com/vol2_no2_t1/Forsythe_Giordano_2011_2_1.pdf

[3] Jonathan D. Moreno, “Can Brain Research Keep Us Safe?”, *Slate*, 8 September 2011 accessed 29 August 2013, http://www.slate.com/articles/technology/future_tense/2011/09/can_brain_research_keep_us_safe.html

[4] Flower, Rod, Dando, Malcolm, Hay, Alastair et all., “Neuroscience, conflict and security”, *The Royal Society*, February 2012, accessed 29 August 2013, http://royalsociety.org/uploadedFiles/Royal_Society_Content/policy/projects/brain-waves/2012-02-06-BW3.pdf.

[5] Rachel Yehuda, Steven E Hyman, ”The Impact of Terrorism on Brain, and Behavior: What We Know and What We Need to Know”, *Neuropsychopharmacology*, No. 30, 2005, pp. 1773-1780 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/ pubmed/16012534 (password required)

[6] Breslau N, Kessler RC, Chilcoat HD et all., “Trauma and posttraumatic stress disorder in the community: The 1996 Detroit Area Survey of Trauma”, *Archives of General Psychiatry*, No. 55, 1998, pp. 626–632 accessed 29 August 2013, http://archpsyc.jamanetwork.com/data/Journals/PSYCH/5056/yoa7340.pdf.

[7] American Psychiatric Association's, “PTSD”, *Diagnostic and Statistical Manual of Mental Disorders V*, 2013, American Psych. Publishing, Arlington, USA accessed 29 august 2013 at http://www.dsm5.org/Documents/PTSD%20Fact%20Sheet.pdf.

[8] Y Neria, L DiGrande, BG Adams, “Posttraumatic stress disorder following the September 11, 2001, terrorist attacks: a review of the literature among highly exposed populations”, *American Psychol.*, September 2011, No. 66(6), pp. 429-446 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3386850/

[9] Duffy M, Gillespie K, Clark DM. “Post-traumatic stress disorder in the context of terrorism and other civil conflict in Northern Ireland: randomised controlled trial”, *British Medical Journal*, 2 June 2007, Vol. 334(7604), pp. 1147-1153 accessed 29 August 2013, http://www.bmj.com/content/334/7604/1147?view=long&pmid=17495988.

[10] S Scrimin, G Axia, F Capello et all., “Posttraumatic reactions among injured children and their caregivers 3 months after the terrorist attack in Beslan”, *Psychiatry Res.*, 30 March 2006, Vol. 141(3), pp. 333-336 accessed 29 August 2013, http://dpss.psy.unipd.it/files/docs/Moscardino/Psychiatry_Research.pdf

[11] S Galea, H Resnick, J Ahern et all., “Posttraumatic stress disorder in Manhattan, New York City, after the September 11th terrorist attacks”, *J Urban Health.*, September 2002, No. 79(3), pp. 340-353 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3456781/pdf/11524_2006_Article_133.pdf

[12] A Ehlers, DM Clark, “A cognitive model of posttraumatic stress disorder”, *Behavior Research and Therapy*, No. 38, 2000, p. 324 accessed 29 August 2013, http://biomagnet.uni-muenster.de/PDF_library/005829.pdf

[13] According to Brown and Kulik (1977), flashbulb memories are vivid, detailed, and long-lasting memories of the circumstances in which people first learned about shocking public events. Flashbulb memories have six characteristic features: place, ongoing activity, informant, own affect, other affect, and aftermath. Most of the studies indicate that flashbulb memories are not more accurate than other types of memories and they are prone to errors and deterioration.

[14] O Luminet, A Curci, EJ Marsh, et. all., "The cognitive, emotional, and social impacts of the September 11 attacks: group differences in memory for the reception context and the determinants of flashbulb memory", *J Gen Psychol.*, No. 131(3), July 2004, pp. 197-224 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/15248591 (password required).

[15] AE Budson, JS Simons, AL Sullivan et all., "Memory and emotions for the September 11, 2001, terrorist attacks in patients with Alzheimer's disease, patients with mild cognitive impairment, and healthy older adults", *Neuropsychology*., No. 18(2), April 2004, pp. 315-327 accessed 29 August 2013, http://sws1.bu.edu/abudson/9-11-01r.pdf

[16] Hirst W, Phelps EA, Buckner RL, et all., "Long-term memory for the terrorist attack of September 11: flashbulb memories, event memories, and the factors that influence their retention", *J Exp Psychol Gen.*, No. 138(2), May 2009, pp. 161-176 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2925254/

[17] Flashbacks are perceptions or images rather than verbal descriptions. They incorporate bodily reactions such as pain. They are experienced in the present, not the past – the patient feels as though they are happening now. They are vivid, and the person becomes involved in the entire experience. Sometimes detail can be seen that is not available in other memories of the incident. Flashbacks are all-or-nothing. They switch on and off, and the person has little control. Sufferers might try consciously to change the events, but that is not possible.(Source: Brewin CR, Dalgleish T and Joseph S. "A dual representation theory of post-traumatic stress disorder", *Psychological Review*, No. 103, 1996, pp. 670-686 accessed 29 August 2013, http://homepage.psy.utexas.edu/homepage/class/psy394U/Bower/13%20Theories%20of%20PTSD/A%20dual%20representat%20Brewin.pdf

[18] D Vlahov, S Galea, H Resnick, et al., "Increased consumption of cigarettes, alcohol, and marijuana among Manhattan residents after the September 11th terrorist attacks", *American Journal of Epidemiology*., No. 155, 2002, pp. 988–996 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/12034577

[19] M. W. Bud Perrine, Kerstin E. E. Schroder, Renée Forester, "The Impact of the September 11, 2001, Terrorist Attacks on Alcohol Consumption and Distress: Reactions to a National Trauma 300 Miles from Ground Zero", *Journal of Studies on Alcohol and Drugs*, Volume 65, Issue 1, January 2004 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/15000498 (password required)

[20] G Stecklov, JR Goldstein,"Terror attacks influence driving behavior in Israel", *Proc Natl Acad Sci USA*., No. 101(40), 5 Octomber 2004, pp. 14551-14556 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC521946/

[21] Garrick Blalock, Vrinda Kadiyali, Daniel H. Simon, "Driving Fatalities After 9/11: A Hidden Cost of Terrorism", *Applied Economics*, Volume 41, Issue 14, 2009, pages 1717-1729 accessed 29 August 2013, http://dyson.cornell.edu/faculty_sites/gb78/ wp/fatalities_120505.pdf.

[22] Lavie Peretz, "Sleep Disturbances in the Wake of Traumatic Events", *New England Journal of Medicine*, Vol. 345, 20 December 2001, pp. 1825-1832 accessed 29 August 2013, http://www.nejm.org/doi/full/10.1056/NEJMra012893

[23] PA Palmieri, Chipman KJ, Canetti D et all., "Prevalence and correlates of sleep problems in adult israeli jews exposed to actual or threatened terrorist or rocket attacks", *Journal of Clinical Sleep Medicine*, Vol. 6(6), 15 December 2010, pp. 557-564 accessed 29 august 2013 at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3014242/

[24] VA Franz, DB Arnkoff, CR Glass et all., "Predictors of the impact of the September 11th terrorist attacks on victims of intimate partner violence", *J Trauma Stress.*, Octomber 2011, No. 24(5), pp. 530-537 accessed 29 August 2013, http://www.ncbi.nlm. nih.gov/pubmed/21882248 (password required).

[25] Guy Stecklov, "Terror in the Bedroom: Terror Attacks and Births in Israel from 2000-2006", accessed 29 August 2013, ftp://ftp.dondena.unibocconi.it/AlpPop2011/Stecklov.pdf

[26] K Bulkeley, TL Kahan, "The impact of September 11 on dreaming" *Conscious. Cogn.*, No. 17(4), December 2008, pp. 1248-1256 accessed 29 August 2013, http://www.scu.edu/cas/psychology/news/upload/2008-Bulkeley-Kahan-Dreams-and-9-11.pdf

[27] Ernest Hartmann, Tyler Brezler "A Systematic Change in Dreams after 9/11/01" *Sleep*, February 2008, No. 31(2), pp. 213-218 accessed 29 august 2013 at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2225570/

[28] RE Propper, R Stickgold, R Keeley, Christman SD., "Is television traumatic? Dreams, stress, and media exposure in the aftermath of September 11, 2001", *Psychol Sci.* No. 18(4), April 2007, pp. 334-340 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/17470259 (password required)

[29] WA Pridemore, A Trahan, MB. Chamlin, "No evidence of suicide increase following terrorist attacks in the United States: an interrupted time-series analysis of September 11 and Oklahoma City", *Suicide and Life Threat Behaviour.*, No. 39(6), December 2009, pp. 659-670 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/20121329# (password required)

[30] J. J. Vasterling, L. M. Duke, K. Brailey, et all., "Attention, learning, and memory performances and intellectual resources in Vietnam veterans: PTSD and no disorder comparisons", *Neuropsychology*, No. 16, 2002, pp. 5-14 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/ pubmed/11853357 (password required)

[31] TC Neylan, MLenoci, J Rothlind, "Attention, learning, and memory in posttraumatic stress disorder", *J Trauma Stress.* No. 17(1), February 2004, pp. 41-46 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2366105/

[32] O Abe, H Yamasue, K Kasai, "Voxel-based diffusion tensor analysis reveals aberrant anterior cingulum integrity in posttraumatic stress disorder due to terrorism", *Psychiatry Res., No.* 146(3), 30 April 2006, pp. 231-242 accessed 29 August 2013, http://www.sciencedirect.com/science/article/ii/S0925492706000059 (password required)

[33] H Yamasue, K Kasai, A Iwanami, "Voxel-based analysis of MRI reveals anterior cingulate gray-matter volume reduction in posttraumatic stress disorder due to

terrorism", *Proc Natl Acad Sci U S A*, No. 100(15), 22 July 2003, pp. 9039-9043 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC166434/

[34] N Kitayama, V Vaccarino, M Kutner, "Magnetic resonance imaging (MRI) measurement of hippocampal volume in posttraumatic stress disorder: a meta-analysis", *J Affect Disord.*, No. 88(1), September 2005, pp. 79-86 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/16033700 (password required)

[35] A Karl, M Schaefer, LS Malta, "A meta analysis of structural brain abnormalities in PTSD", *Neurosci Biobehav Rev.*, No. 30(7), 2006, pp. 1004-1031 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/16730374

[36] B Pfefferbaum, P Tucker, CS North, "Autonomic reactivity and hypothalamic pituitary adrenal axis dysregulation in spouses of Oklahoma City bombing survivors 7 years after the attack", *Compr Psychiatry.*, No. 53(7), Octomber 2012, pp. 901-906 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3526068/

[37] R Yehuda, G Cai, JA Golier, "Gene expression patterns associated with posttraumatic stress disorder following exposure to the World Trade Center attacks", *Biol Psychiatry.*, No. 66(7), 1 Octomber 2009, pp. 708-711 accessed 29 August 2013, http://www.cipps.it/docs/[2009]_Gene_Expression_Patterns_Associated_with_Posttraumatic_Stress_Disorder_Following_Exposure_to_the_World_Trade_Center_Attacks.pdf

[38] R Yehuda, LM. Bierer , "The relevance of epigenetics to PTSD: implications for the DSM-V", *J Trauma Stress.*, No. 22(5), Octomber 2009, pp. 427-434 accessed 29 August 2013, http:// www.ncbi.nlm.nih.gov/pmc/articles/PMC2891396/.

[39] SA Maddox, GE Schafe, KJ. Ressler , "Exploring epigenetic regulation of fear memory and biomarkers associated with post- traumatic stress disorder", *Front Psychiatry.*, No. 62(4), July 2013, pp. 62-68 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3697031/

[40] SG Matthews, DI. Phillips, "Minireview: transgenerational inheritance of the stress response: a new frontier in stress research", *Endocrinology.*, No. 151(1), January 2010, pp. 7-13 accessed 29 August 2013, http://endo.endojournals org/content/151/1/7.full

[41] DM Dietz, Q Laplant, EL Watts, "Paternal transmission of stress-induced pathologies", *Biol Psychiatry.*, No. 70(5), 1 September 2011, pp. 408-414 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3217197/

[42] SR Brand, SM Engel, RL Canfield, R. Yehuda, "The effect of maternal PTSD following in utero trauma exposure on behavior and temperament in the 9-month-old infant", *Ann N Y Acad Sci.*, No. 1071, July 2006, pp. 454-458 accessed 29 August 2013, http://onlinelibrary.wiley.com/doi/10.1196/annals.1364.041/abstract (password required)

[43] Patrice van Eersel, Catherine Maillard, "Ma dor stramosii", pp. 20-24, Editura Philobia, 2011, Bucuresti.

[44] LV. Harper, "Epigenetic inheritance and the intergenerational transfer of experience", *Psychol Bull.*, No. 131(3), May 2005, pp. 340-360 accessed 29 August 2013, http://psycnet.apa.org/journals/bul/131/3/340/

[45] NATO Science and Technology Organization "Psychosocial, Organizational and Cultural Aspects of Terrorism, Chapter 15 – Modeling psycho-social resilience to terrorism", November 2011 accessed 29 august 2013, http://www.cso.nato.int/pubs/rdp. asp?RDP=RTO-TR-HFM-140

[46] Mary Marshall Clark "The September 11, 2001, Oral History Narrative and Memory Project: A First Report The Journal of American History", *History and September 11: A Special Issue*, Vol. 89, No. 2, September 2002, pp. 569-579 accessed 29 August 2013, http://www.jstor.org/stable/3092175

[47] E Ullmann, A Barthel, J Licinio, et all., "Increased rate of depression and psychosomatic symptoms in Jewish migrants from the post-Soviet-Union to Germany in the 3rd generation after the Shoa", *Translational Psychiatry*, 2013 Mar 12, No. 241, accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625916/

[48] J Bohacek, K Gapp, BJ Saab, IM. Mansuy, "Transgenerational epigenetic effects on brain functions", *Biol Psychiatry*, Vol. 73(4), 15 February 2013, pp. 313-320 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/23062885 (password required)

[49] WA Tol, C Barbui, M. van Ommeren, "Management of acute stress, PTSD, and bereavement: WHO recommendations", *JAMA*, Vol. 310(5), 7 August 2013, pp. 477-488 accessed 29 August 2013, http://jama.jamanetwork.com/article.aspx?articleid=1724282

[50] S Schreiber, OT Dolberg, G Barkai, et all., "Primary intervention for memory structuring and meaning acquisition (PIMSMA): study of a mental health first-aid intervention in the ED with injured survivors of suicide bombing attacks", *Am J Disaster Med*.,No. 2(6), Nov-Dec 2007, pp. 307-320 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/18297951

[51] BV Watts, PP Schnurr, L Mayo, Young-Xu Y, et all., "Meta-analysis of the efficacy of treatments for posttraumatic stress disorder", *J Clin Psychiatry*, No. 74(6), June 2013, pp. 541-550, accessed 29 August 2013, http://article.psychiatrist.com/dao_1-login.asp?ID=10008306&RSID=65831712447946

[52] C Andrade, D Mushtaq, MA. Margoob, "Electroconvulsive therapy for posttraumatic stress disorder: the importance of assessment measures" *J ECT*., No. 27(4), December 2011, pp. 341-352 accessed 29 August 2013, http://journals.lww.com/ectjournal/Citation/2011/12000/Electroconvulsive_Therapy_for_Posttraumatic_Stress.21.aspx (password required)

[53] Adam J. Kolber, "Therapeutic Forgetting: The Legal and Ethical Implications of Memory Dampening", *Vanderbilt Law Review*, Vol. 59, 2006, p. 1579 accessed 29 August 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=887061

[54] *Idem*, p. 1598.

[55] *Idem*, pp. 1603-1604.

[56] S. Matthew Liao, Anders Sandberg, "The Normativity of Memory Modification", *Neuroethics*, No. 85(1), 2008, pp.85-99 accessed 29 August 2013, http://www.fhi.ox.ac.uk/wp-content/uploads/normativity-of-memory-modification.pdf

[57] JJ Day, JD. Sweatt, "Cognitive neuroepigenetics: a role for epigenetic mechanisms in learning and memory", *Neurobiol Learn Memory*, July 2011, No. 96(1), pp. 2-12 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3111867/

[58] EB. Keverne "Significance of epigenetics for understanding brain development, brain evolution and behavior", *Neuroscience*, 29 November 2012, No. 12, pp. 1141-1144 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pubmed/23201253 (password required)

[59] Erik Parens, "The Ethics of Memory Blunting and the Narcissism of Small Differences", *Neuroethics*, Volume 3, Issue 2, July 2010, pp. 99-107 accessed 29 August 2013, http://www.thehastingscenter.org/uploadedFiles/About/People/Staff/Memory%20Blunting%20and%20Narcissism%20of%20Small%20Differences.pdf

[60] Daniel Kimmage, "The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message", *Radio Free Europe/Radio Liberty*, No. 4, March 2008, pp. 4-6, accessed 29 August 2013, http://www.e-prism.org/images/AQ_Media_Nexus_-_March08.pdf

[61] Catherine Booh, James Castan, Robertson Dikens et all., "Recruitment and radicalization of school-aged youth by international terrorist groups", Final raport, *Homeland Security Institute*, 23 April 2009, accessed 29 August 2013, http://www.cleanitproject.eu/wp-content/uploads/2012/07/2009-recruitment-and-radicalization.pdf

[62] Catherine C. Marshall, "How People Manage Information over a Lifetime", 2006, p. 3 accessed 29 August 2013, http://www.csdl.tamu.edu/~marshall/PIM%20Chapter-Marshall.pdf

[63] Cristian Barna, "Jihad in Europa – Amenintarea terorista de franciza "Al-Qaida", *Revista Intelligence*, No. 19, Martie-Mai 2011, pp. 12-17 accessed 29 August 2013, http://www.sri.ro/upload/intelligencemartie2011.pdf

[64] Institute for Strategic Dialogue, "Radicalisation: The role of the Internet", Working Paper, 2011, accessed 29 August 2013, http://www.strategicdialogue.org/StockholmPPN2011_BackgroundPaper_FOR%20WEBSITE.pdf

[65] Steven R. Corman, "Understanding Extremists‟ Use of Narrative to Influence Contest Populations", presented at Workshop on Mapping Ideas: Discovering and Information Landscapes, June 2011, p. 1 accessed 29 August 2013, http://mappingideas.sdsu.edu/old_Mappingideas/SummerWorkshop/2011/Papers/Corman_Position.pdf

[66] Sarah Canna, Carley St. Clair, Abigail Chapman," Neurobiological & Cognitive Science Insights on Radicalization and Mobilization to Violence: A Review", June 2012 accessed 29 August 2013, http://mappingideas.sdsu.edu/publications/Theories%20of%20Radicalization_Gupta.pdf

[67] O.Ashour., "The Deradicalization of Jihadists: Transforming Armed Islamist Movements", Routledge, 2009, London, pp. 4-7.

[68] O. Ashour, *op. cit.*, pp. 138-142.

[69] Harold Hawkins, Richard Davis, Scott Atran, et all., “Theoretical Frames on Pathways to Violent Radicalization”, ARTIS, August 2009, p. 8 accessed 29 August 2013, http://www.artisresearch.com/articles/ARTIS_Theoretical_Frames_August_2009.pdf

[70] DARPA, accessed 29 August 2013, http://www.darpa.mil/Our_Work/DSO/Programs/Narrative_Networks.aspx

[71] George Dvorsky, “Propaganda 2.0 and the rise of „narrative networks‟”, *h+* online edition, 16 November 2011 accessed 29 August 2013, http://hplusmagazine.com/2011/11/16/propaganda-2-0-and-the-rise-of-narrative-networks/

[72] IARPA site, accessed 29 August 2013, http://www.iarpa.gov/Programs/ia/Metaphor/metaphor.html

[73] IARPA site, accessed 29 August 2013, http://www.iarpa.gov/Programs/ia/ICArUS/icarus.html

[74] Joe Fassler, “Can the Computers at Narrative Science Replace Paid Writers?”, The Atlantic-online edition, 12 April 2012, accessed 29 August 2013, http://www.theatlantic.com/entertainment/archive/2012/04/can-the-computers-at-narrative-science- replace-paid-writers/255631/

[75] G. J. Neimeyer & A. E. Metzler, “Personal identity and autobiographical recall” in U. Neisser & R. Fivush, “Remembering self: The construction and accuracy in the self-narrative”, Cambridge University Press, 1994, pp. 105–135 accessed 29 August 2013, http://ebooks.cambridge.org/chapter.jsf?bid=CBO9780511752858&cid=CBO9780511752858A014(password required)

[76] M. L. Howe., “The Adaptive Nature of Memory and Its Illusions”, *Current Directions in Psychological Science*, No. 20 (5), 2011, p. 312 accessed 29 August 2013, http://cdp.sagepub.com/content/20/5/312.full.pdf+html (password required)

[77] Baym CL, Gonsalves B., “Comparison of neural activity that leads to true memories, false memories, and forgetting: an fMRI study of the misinformation effect”, Cognit. Affect. Behav. Neurosci., No. 10, 2010, pp. 339–348 accessed 29 August 2013, https://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CEgQFjAC&url=http%3A%2F%2Fmoodle.ncku.edu.tw%2Fmod%2Fresource%2Fview.php%3Fid%3D47269&ei=eqklUrfUO4OXtAaJwoDIBg&usg=AFQjCNFersxgn59G5Nzh1PUm31OcGsDeHg&sig2=8mgLEUcHhCOg5YTaaMaK9g&bvm=bv.51495398,d.Yms.

[78] Schacter DL, Guerin SA, St Jacques PL., “Memory distortion: an adaptive perspective”, *Trends Cogn Sci.*, No. 15(10), Octomber 2011, pp. 467-474 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3183109/

[79] DL Schacter, et al., “Remembering the past to imagine the future: the prospective brain”, *Nat. Rev. Neurosci,*. No. 8, 2007, pp. 657-661 accessed 29 August 2013, http://www.wjh.harvard.edu/~dsweb/pdfs/07_01_DRA_ATW_DLS.pdf.

[80] Echterhoff, G., Higgins, E. T., & Levine, J. M., “Shared reality: Experiencing commonality with others‟ inner states about the world”, *Perspectives on Psychological Science*, 2009, No. 4, pp. 496-521 accessed 29 August 2013, http://www.lrdc.pitt. edu/pubs/Abstracts/EchterhoffShared.pdf

[81] Benjamin C. Storm et all., "Accelerated Relearning After Retrieval-Induced Forgetting: The Benefit of Being Forgotten", *Journal of Experimental Psychology*, 2008, Vol. 34, No. 1, pp. 230-236 accessed 29 August 2013, http://psycnet.apa.org/ journals/xlm/34/1/230/ (password required)

[82] A Clark, RA Nash, G Fincham, G. Mazzoni, "Creating non-believed memories for recent autobiographical events", *PLoS One.*, No. 7(3), 2012 accessed 29 August 2013, http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0032998

[83] CB Stone, AJ Barnier, J Sutton, W. Hirst, *op. cit.*, p. 2.

[84] A Coman, W. Hirst, "Cognition through a social network: the propagation of induced forgetting and practice effects", *J Exp Psychol Gen.*, No. 141(2), May 2012, pp. 321-36 accessed 29 August 2013, http://www.princeton.edu/~acoman/ Publications_files/Coman%20%26%20Hirst%20(2011)-JEPG.pdf.

[85] SJ Barber, M. Mather, "Forgetting in context: the effects of age, emotion, and social factors on retrieval-induced forgetting", *Mem Cognit*, No. 40(6), August 2012, pp. 874-888 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/ pmarticles/PMC3594662/

[86] W. Hirst, "The contribution of mnemonic malleability to collective memory", 2010, In P. A. Reuter -Lorenz, K. Baynes, G. R. Mangun, & E. A. Phelps (Eds.), "The cognitive neuroscience of the mind: A tribute to Michael S. Gazzaniga", MIT Press., 2010, pp. 139-154 *apud* CB Stone, AJ Barnier, J Sutton, W. Hirst "Forgetting Our Personal Past: Socially Shared Retrieval-Induced Forgetting of Autobiographical Memories", *J Exp Psychol Gen.*, 12 November 2012, pp. 1-17 accessed 29 August 2013, http://www.johnsutton.net/Stone_Barnier_Sutton_ Hirst_2013.pdf.

[87] M Fernandes, J. Saunders "Does retrieval-induced forgetting affect future social behavior?", *Acta Psychol (Amst).*, No. 144(1), September 2013, pp. 1-5 accessed 29 August 2013, http://www.sciencedirect.com/science/article/pii/ S0001691813000978

[88] A Coman, D Manier, W. Hirst, "Forgetting the unforgettable through conversation: socially shared retrieval induced forgetting of September 11 memories", *Psychol Sci.*, No. 20(5), May 2009, pp. 627-633 accessed 29 August 2013, http://www.princeton.edu/~acoman/Publications_files/Coman,%20Manier, %20%26%20Hirst%20(2009)-Psychological%20%20Science.pdf

[89] S Lee, VC Ramenzoni, P. Holme, "Emergence of collective memories", *PLoS One.*, No. 5(9), 1 September 2010, pp. 1-16 accessed 29 August 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2931705/

[90] A. F. Lemieux, "The role and impact of music in promoting (and countering) violent extremism in countering violent extremism", *Interagency White Paper*, Ed. Laurie Fenstermacher, 2011, pp. 147-157 accessed 29 August 2013, http://lemieux.socialpsychology.org/publications.

[91] Hamm, "Prisoner radicalization: Assessing the threat in U.S. correctional institutions", 2008, p. 17 *apud* Sarah Canna, Carley St. Clair, Abigail Chapman,"

Neurobiological & Cognitive Science Insights on Radicalization and Mobilization to Violence: A Review", June 2012, p. 24 accessed 29 August 2013, http://mappingideas.sdsu.edu/publications/Theories%20of%20 Radicalization _Gupta.pdf

[92] A. F. Lemieux, *op. cit.*, p. 152 accessed 29 August 2013, http://lemieux.socialpsychology.org/publications

[93] LR Slevc, JC Rosenberg, AD Patel, "Making psycholinguistics musical: self-paced reading time evidence for shared processing of linguistic and musical syntax", *Psychon Bull Rev.*, No. 16(2), 16 April 2009, pp. 374-381, accessed 29 August 2013, thttp://www.ncbi.nlm.nih.gov/pmc/articles/PMC2658747/

[94] P Perruchet, B. Poulin-Charronnat, "Challenging prior evidence for a shared syntactic processor for language and music", *Psychon Bull Rev.*, No. 20(2), April 2013, pp. 310-317 accessed 29 August 2013, http://link.springer.com/article/10.3758%2Fs13423-012-0344-5

[95] J Jolij, M. Meurs, "Music alters visual perception", *PLoS One.*, No. 6(4), 21 April 2011, pp. 1-10, accessed 29 August 2013, at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3080883/

[96] C., Kirchhübel, D. M. Howard, "Investigating the acoustic characteristics of deceptive speech", *Proceedings of the 17th International Congress of Phonetic Sciences, Hong Kong*, 2011, pp. 1094-1097 accessed 29 August 2013, http://www.icphs2011.hk/resources/OnlineProceedings/RegularSession/Kirchhubel/Kirchhubel.pdf

[97] M Garry, KA. Wade, "Actually, a picture is worth less than 45 words: narratives produce more false memories than photographs do", *Psychon Bull Rev.*, No. 12(2), April 2005, pp. 359-366 accessed 29 August 2013, http://www.ncbi.nlm. nih.gov/pubmed/16082819 (password required)

[98] RA Nash, KA Wade, RJ. Brewer, "Why do doctored images distort memory?", *Conscious Cogn.*, No. 18(3), September 2009, pp. 773-780 accessed 29 August 2013, http://wrap.warwick.ac.uk/1061/1/WRAP_Wade_nash-wade-brewer-inpress.pdf

[99] D Strange, M Garry, DM Bernstein, DS. Lindsay,"Photographs cause false memories for the news", *Acta Psychol (Amst).*, No. 136(1), January 2011, pp. 90-94 accessed 29 August 2013, http://web.uvic.ca/~dslind/sites/default/files/Strange,Garry,Bernstein,&Lindsay2010.pdf

[100] Dario L.M. Sacchi, Franca Agnoli, Elizabeth Loftus, "Changing History: Doctored Photographs Affect Memory for Past Public Events", *Applied Cognitive Psychology*, No. 21, 2007, pp. 1020-1021 accessed 29 August 2013, https://webfiles.uci.edu/ eloftus/Sacchi_Agnoli_Loftus_ACP07.pdf

[101] Nash RA, Wade KA, Lindsay DS., "Digitally manipulating memory: effects of doctored videos and imagination in distorting beliefs and memories", *Mem Cognit.*, No. 37(4), June 2009, pp. 414-424 accessed 29 August 2013, http://web.uvic.ca/~dslind/ sites/default/files/Nash,Wade,&Lindsay2009.pdf

[102] Garoff-Eaton RJ, Slotnick SD, Schacter DL., "Not all false memories are created equal: the neural basis of false recognition", *Cereb Cortex.*,

No. 16(11), November 2006, pp. 1645-1652 accessed 29 August 2013, http:// cercor.oxfordjournals.org/ content/16/11/1645.long

[103] Gary Lupyan, Michael J. Spivey, "Language can boost otherwise unseen objects into visual awareness", *PNAS*, published online before print 12 August 2013 accessed 29 August 2013, http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0011452

[104] Hwiman Chung, Euijin "The Effects of Web Site Structure: The Role of Personal Difference", *Ahn. CyberPsychology & Behavior*, December 2007, Volume: 10 Issue 6, pp. 749-756 accessed 29 August 2013, http://online.liebertpub.com/doi/pdf/10.1089/cpb.2007.9955

[105] Sebastian Seung, "Another Perspective on Massive Brain Simulations", *Scientific American – online edition*, 11 June 2012, accessed 29 August 2013, http://www.scientificamerican.com/article.cfm?id=massive-brain-simulators-seung-conntectome& page=2.

[106] Carsten Detken, "Is Early Warning Against Systemic Risk Feasible?", *FuturICT site*, 14 January 2013, accessed 29 August 2013, http://www.futurict.eu/carsten-detken-early-warning-against-systemic-risk-feasible

The New Virology Becoming Viral: Germs and Pixels's Game in Intelligence Sharing

Gabriela-Cornelia HOROŞANU[*]

Abstract

In the context of emerging global threats, which are asymmetric and versatile, the issue of intelligence sharing and the need for an institutionalised transnational collaboration in the field of disease surveillance and cyber attacks monitoring is becoming a focal point in governmental discussions.

The overall objective of the current study is bringing two large and complex emerging threats together with the purpose of describing their common features and the similar difficulties to detect, report, and control each one of them. This study proposes a risk assessment methodology for detection and control of potentially catastrophic outbreaks, such as pandemics and cyber attacks with physical consequences. Intelligence sharing is praised in the article as the a priori factor in monitoring the transnational challenges of the most dangerous current ‚covert agents'. These are two different types of viruses: one targeted on men, the other one on computers. In a time when using asymmetric threats became the rule of thumb in conducting an attack, decision makers need different kind of intelligence products. Using the interdependence theory, the study shows that, when warnings of worldwide infections with germs and cyber viruses seem like monthly occurrences and their proliferation is difficult to control and to trace back, in order to detect and report them in real-time, reliable sources and targeted global intelligence sharing is needed.

Keywords: epidemics, cyber attacks, risk assessment, forensics, transnational challenges

In the current world, among several emerging and challenging threats, two of them, having nothing in common in the physical world, share the same strategy of spreading themselves and attack before their targets could realise that. One comprised of bits of electronic data, digitally encoded, the other one comprised of chromosomes with biological data, with an ARN-based code but they are both being generically called viruses.

Viruses are simultaneously the oldest and the youngest beings on Earth and the biggest natural threat to humanity since ever. As the simplest organisms they have transformed themselves and became easily adapted to the environment, the human immune systems, and the antivirals. Generations of viruses have emerged and then re-emerged more powerful after centuries of inactivity. Lately, triggered by the globalisation phenomenon, which subsequently

[*] PhD, Ministry of Health, Romania

brought racial mixes, easy and affordable transportation, states interdependence and boundaries relaxation, the viral strains have combined and gave birth to extremely resistant and lethal viruses. These germs are easily transmitted through breath or body fluids from person to person or, even more hazardous, from animals to humans (commonly know as *zoonosis*). Some very easily prepared and spread bring forward their utility as a weapon now more than ever, handy for terrorist groups or rogue states. Their biggest advantage is their 'invisibility cloak' and their 'covert agents' attitude-like. Some human bodies are used just as 'transport' means, as 'spreading agents', therefore the proliferation is difficult to control as the symptoms show up after the active infection. Advances in technology and medicine can now help predict some of the known epidemics. Globalisation plays here a good role, improving information sharing and pandemics awareness, as it will be described later in this study.

Advanced technologies does not offer just benefits but also raise new challenges, such as cyber threats. Once the common systems become more and more digitalised, they also become more interdependent and more vulnerable to attacks. Thus, a new type of virus was born, the cyber one. Sharing the same name, generically, despite the one made by nature to infect humans, this one was made by man to infect computers. Their purpose and their effects are similar, both catastrophic for humanity, both difficult to predict and prevent, both transnational threats.

In the current study common features of the two viral species will be presented, with a further view on their threat risk assessment, and the tradecraft methodology, which is currently in use or could be used to better predict and prevent these threats. The hypothesis is that progress in these domains can be achieved only by collective action, with common standard procedures of risk assessment and information sharing, due to the high interdependence of states regarding these threats.

Knowing the enemy

Euphemistically described, the two types of viruses live in a type of cloud, floating parallel with people and sometimes discharging and affecting our lives. Computer networks are a part of a *sui generis* world, a virtual world by definition, paradoxically easy and difficult to monitor, control and protect. Natural germs, due to their microscopic dimensions, are invisible to humans in normal conditions. This offers the advantage of free and uncontrollable moving of these viruses. Victory is easily achieved by knowing the enemy. In this case, the system of equations that could help predict their behaviour have more unknown variables than equations. It is a non-linear system, which can be described by a fuzzy approach, providing just a broad perspective of effects and offering some confidence boundaries for action.

The generic name of 'viruses' for the two phenomena came with similarities between the two of them, such as the 'invasion' technique. They follow the same strategic steps: replicate, hide, destroy, and evade the host.

Research in the biological sciences undertaken for the purpose of weaponing biological agents so that they can be used to kill or cause illness in human populations is presumably morally impermissible, whether the research in question is undertaken by state actors, (non-state) terrorist groups, criminal organizations or malevolent individuals.

Biological warfare has been practiced for thousands of years, but the use of modern biological weapons (BWs) has been very limited. In essence, BWs include a living pathogen, a virus, for example, or a toxin produced by living organism. Weapons including a living pathogen are more difficult to store and deliver than toxins are, because there must be assured special conditions, in order to ensure that the pathogen does not die before infecting its target; that is why, an agent like this must be robust. Another important characteristic of the BW agent are the infectivity – the smaller the amount of agent required to infect an individual, the higher its infectivity, the pathogenicity – the percentage of individuals manifesting the symptoms of a disease to which they have been exposed, the virulence – the severity of a particular disease, and the incubation period – which determines the degree of spreading the disease.

The biological agents of most concern are smallpox and haemorrhagic fever viruses, botulinum toxin, anthrax, tularemia and plague bacteria.[1]

Not all BWs facilitate the spread of communicable diseases. For example, biological agents such as anthrax and botulinum toxin do not cause diseases that are typically spread by personal contact. Thus, an outbreak of disease is inherently limited. On the other hand, there are also biological agents that do spread communicable disease, as Q fever, bubonic plague and smallpox.

Also, a perturbing factor in analysis and prediction is the fact that those who carry or spread the disease behave differently. In epidemics such as SARS what might be termed "super-spreaders" play an inordinate role. A famous super-spreader was an Irish cook in New York, Mary Mallon, more commonly known as "Typhoid Mary" who never suffered from typhoid herself but transmitted it to the families she cooked for. More recently during the SARS epidemic, several people were identified who had passed on the disease to a surprisingly large number of other individuals. Frequent travelling during a period in which the disease is particularly virulent and susceptible to transmission from person to person and symptoms such as coughs and sneezes, which transmit the disease to people in close proximity, are proliferation factors for infectious diseases.[2]

While some diseases occur easily in nature and are highly contagious, others require sophisticated processing for use as a weapon. Weaponing pathogens and disseminating them in the air is extremely difficult, lesson that has been painfully learned by Saddam Hussein's scientists. The sequencing machines are improving their capacity and becoming smaller and cheaper every year. With the rise of synthetic biology, a relatively new field using engineering techniques to create new biological parts, devices, or systems, or redesign existing ones, fears of its terrorist use have escalated. New pandemics can start being developed with the help of developing synthetic biology technique. Also, current developments in nanotechnology start to show a new face, bringing forward the threat of small, targeted armies, which could be injected or dispersed in aerosols, invading bodies as powerful epidemics, not just curing their diseases.

Cyber attacks on the other hand have a more diverse area of action, starting from exploitations to steal money or data, disruptions, such as distributed denial-of-service, or espionage activities. These attacks vary much as they come on three levels, as they were defined at the NATO Cyber Security Roundtable in 2011: garden variety, mercenary, and nation state, the latest coming with a very sophisticated tradecraft. Multistage cyber attacks are more elaborated and harder to trace back, as a malware penetrates a computer to use it as a platform for infecting another machines.

At a first glance, preventing these treats looks like an almost impossible mission. Nevertheless, there are methods of profiling the viruses' shapes and behaviours. In a manner of speaking, viruses can be 'spied' just like humans can; you can 'enter in their heads and foreseen their possible actions. It is a strange approach, but just like the human mind can be able to produce an infinite number of thoughts, depending on a great number of variables, so does the viruses can proceed. Nevertheless, so as the human beings react on specific patterns because no matter the thoughts, these are the only possible ways of reacting (because of the universal laws' boundaries, for example), the same happens to the natural of cyber viruses. Predictive patterns can be thus built, usually following their precedent actions and a 'first flag' left on a victim.

The difficulty is yet raised but the difficulty to trace back the attacks, both in the biological and cybernetic worlds. Another current problem is that on the Internet one can easily find attack codes, which can be copied and used as blueprint for developing a new generation of cyber viruses. In a similar manner, Internet also offers room for biological viruses recipes, advices for preserving and spreading them, and, obviously, about their effects. Unlike conventional weapons, these weapons can be copied. And their proliferation cannot be easily controlled.

Still, the comparison approach of the two threats provided at least one way of solving these problems. The biggest fear of a biological virus is the immune system. When countering a dangerous pathogen, part of the immune system adapts and is able to resist the invader even if it was unknown before. In the cyber world, an immune system can be created by a "learning algorithm" that would allow them to adapt and resist to new attacks. Artificial intelligence is comprised of learning algorithms based on genetic approach, for example. These are called genetic algorithms and optimize the behaviour of a system using the main rules of genetic evolution, such as population resistance and gene domination.

Monitoring and countering threats

Mechanisms of surveillance, monitoring and reporting of these two categories of threats are developed both nationally and internationally, due to the high degree of interdependence between nations and network when countering these threats.

Although in the cyber space nations try to currently develop legislation and interoperable regulations, the biological domain proved that treaties couldn't do much in such difficult to control environments. A global treaty banning germ warfare was settled in 1972 and has only 163 signatories, less than the one on nuclear non-proliferation treaty (189) and the chemical weapons banning treaty (188).[3]

At the international level, in cooperation with governments, WHO develops norms and standards, guidance and public health tools to help countries implement effective disease prevention and control programmes and address their risk factors. Inside WHO, the Global Outbreak Alert and Response Network (GOARN) provides an operational framework to link national expertise and skill to keep the international community constantly alert to the threat of outbreaks and ready to respond. Disease outbreak news are daily updated on the WHO Global Alert and Response (GAR) webpage. Currently, Middle East respiratory syndrome coronavirus (MERS-CoV) and human infection with avian influenza A(H7N9) virus cases are considered of concern and daily reported according to the International Health Regulations. The former is similar to the virus responsible for the SARS outbreak in 2002 and 2003 and has, since 2012, infected 64 people, 38 of them fatally. Influenza A H7N9 is a virus that normally circulates in birds but has, since the beginning of 2013, infected 137 people, 32 of them fatally.[4]

Epidemic intelligence is a part of GAR and pursues systematic event detection. WHO global alert and response systematically gathers official reports and rumours of suspected outbreaks from a wide range of formal and informal sources. Formal reports of suspected outbreaks are received from ministries of health, national institutes of public health, WHO Regional and Country offices, WHO collaborating centres, civilian and military laboratories, academic institutes, and nongovernmental organizations (NGOs). In order to ensure a comprehensive picture of the epidemic threat to global health security, WHO also gathers epidemic intelligence from all informal sources, such as the electronic media and electronic discussion groups. In this respect, the Global Public Health Intelligence Network (GPHIN), developed by Health Canada in collaboration with WHO, is a secure Internet-based multilingual early-warning tool that continuously searches global media sources such as news wires and web sites to identify information about disease outbreaks and other events of potential international public health concern. More than 60% of the initial outbreak reports come from unofficial informal sources, including sources other than the electronic media, which require verification.[5]

In responding to an emerging cross-border health threat, the first crucial step is to assess the risks. For both types of viruses common procedures for risk assessment have to be established, especially between highly interconnected societies, such as the European Member States.

Following the example of the United States, where Centers for Disease Control and Prevention (CDC) [www.cdc.gov] currently monitor infectious diseases, have developed an Epidemic Intelligence Service, and raise awareness through an Emergency and Response mechanism, the EU Member States have developed an European Centre for Disease Prevention and Control (ECDC).[6]

Also, the European Commission's Health Security Initiative is designed to put in place efficient risk assessment mechanisms. In 2005, DG SANCO launched regular meetings of Chairs and Secretariats of the Scientific Committees and Panels of Community bodies involved in risk assessment as a standing forum for facilitating the sharing of best practices between risk assessors. The objective is to develop a common approach, containing general principles and engagement with stakeholders and clear and effective risk communication by using a consistent and clear terminology, a clear description of the scope and nature of risks, uncertainties and their implications. Nevertheless, a framework for EU and international co-operation is currently developed, including procedures for the data exchange and information sharing.

Consequently, on 3rd July 2013, The European Parliament adopted the Commission proposal for a Decision on serious cross-border threats to health and on 19th July 2013 the Council has approved the Decision. The adoption of this Decision will help Member States to prepare for and to protect citizens against possible future pandemics and serious cross border threats caused by communicable diseases, chemical, biological or environmental events.[7]

An EU sponsored project, the "Integrated Mobile Security Kit" (IMSK), began in March 2009 and finalized this year, provides a way to combine technologies for area surveillance, checkpoint control and the detection of CBRNE (chemical, biological, radiological, nuclear, explosive) threats. The technologies' sensor data was fed into a single information platform via a secure communication module and then fused to create a common picture, which could be rapidly distributed. Sensors for CBRNE detection, 3D face recognition and detection of hidden weapons via passive THz technology were also developed during this project.[8]

Several initiatives were taken to create joint platforms of real-time news alert systems focuses on diseases and bioterrorism, such as the Medical Information System (Medisys) platform.[9]

In a similar way, Computer Emergency Response Teams (CERTs) are monitoring cyber vulnerabilities and assess their risk.

The EU Member States monitor the cyber threats and collect them through the CERT systems on the EU-CERT platform. A permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies has been established on September 11th 2012. The team is made up of IT security experts from the main EU Institutions and it cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies. Latest news concerning vulnerabilities, threats and techniques are daily collected and updated and targeted Security Advisory are currently posted. Unfortunately, no threat profiles or risk assessment is conducted jointly at the EU level and CERT-EU evaluates threats only targeted on EU Institutions.[10]

With a slight different approach, the US-CERT Cyber Security Bulletin provides a weekly summary of new vulnerabilities.[11]

On the other hand, the European Network and Information Security Agency (ENISA) is analysing the major cyber attacks and is publishing annually a major incidents report, a threat landscape, and specific risk assessments (for example, on cloud computing). The ENISA Threat Landscape (8 January 2013) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. An inventory of methods, tools, and good practices for risk management is also posted on their website.[12]

The main issue is that in both field, biologic and cybernetic, surveillance, response, and communication capabilities vary greatly among states. Standards and procedures are sometimes very difficult to turn interoperable in sensitive field, similar to the status of the intelligence sharing process across nations and agencies.

Risk assessment and tradecraft methodology

As in HUMINT or as on a chessboard, it takes time to study the adversary's moves, prepare for action, foreseen the purpose, wait for a mistake. But viruses are rapidly moving, covertly spreading through population or networks, usually without any warning. Still, if targets are known and their vulnerabilities studied, highly efficient fences can be built. Awareness has a key role in this endeavour and it can be achieved only through highly efficient information sharing and collecting mechanisms between different stakeholders in society and by specific targeted procedures at the international level.

Also, as mentioned above, risk assessment and tradecraft becomes even more difficult to build because of the forensic difficulty, as tracing back the perpetrator in both cases is very challenging, leaving neither reasonable 'fingerprints' nor clues. Tradecraft is tedious in this respect as reliable sources of information are difficult to find and the information hard to be verified or checked twice. This makes detection and reporting in real-time almost impossible, as both kinds of attacks are usually noticed after start spreading.

In both cyber and biological fields risk assessment has to include a common terminology, a collection of information about threat agents and attack vectors, the impact predicted and achieved on different targets, the analysis of potential scenarios accommodating emerging threat trends.

Playing defence is difficult because defender has to find all the vulnerabilities that could be exploited, but the attacker has to find only one and it also has on its side the surprise effect. In reality, attackers usually take the path of least resistance and use tried and proven techniques. By getting to know these techniques, one can understand and counterfeit their tradecraft.[13]

Transmission of infectious diseases depends on various factors, including climate and environment. Diseases sent by food and water, for example, are associated with high temperatures. Disease transmitting vectors (e.g, mosquitos, sand fleas, and ticks) are very sensitive to climatic conditions, temperature and humidity included; their geographic distribution will increase with the climate changes, potentially offering them the possibility to spread in regions where nowadays are incapable of living. Reducing the effects of transmissible diseases linked to climatic changes needs continuous epidemiological surveillance, as well as preparedness for immediate epidemiological measures in order to answer to these threats. Also, one must consider the investigation of the transport routes and the improvement of the drinking water and alimentation safety, the monitoring of insects and other vectors transmitting diseases, both with the insurance of a rapid answer to the public heath section, in case of infection nests.

Traditionally, epidemiology has been based on data collected by public health agencies through health personnel in hospitals, doctors' offices, and out in the field. In recent years, however, novel data sources have emerged where data are frequently collected directly from individuals through the digital traces they leave as a consequence of modern communication and an increased use of electronic devices. Digital data sources can provide local and timely information about disease and health dynamics in populations around the world. [14]

FluNet, for example, is a global tool developed by WHO for influenza virological surveillance. The virological data entered into FluNet are critical for tracking the movement of viruses globally and interpreting the epidemiological data. The data is publically available, it is real-time provided and the results are presented in various formats including tables, maps and graphs. The data are provided remotely by National Influenza Centres (NICs) of the Global Influenza Surveillance and Response System (GISRS) and other national influenza reference laboratories collaborating actively with GISRS, or are uploaded from WHO regional databases.[15]

Bringing the cyber and the biological field together does not offer just possible behavioral patterns but also joint, interdisciplinary tools, such as digital epidemiology. It raised as a new field of increasing importance for tracking infectious disease outbreaks and epidemics by leveraging the widespread use of the Internet and mobile phones. It already played a crucial role in the surveillance of both Middle East Respiratory Syndrome Coronavirus and Avian Influenza A H7N9 by enhancing transparency and helping public health officials to better understand outbreaks. Data from social media and mobile-phones conversations, filtered by data-mining techniques, can predict dynamics of disease spreading.[16]

The researchers from the Romanian National Research and Development Institute Cantacuzino have already mentioned their openness to this method of epidemics tracking.

Although this methodology is revolutionary and it could prove highly effective, the international context seems sensitive to any type of over surveillance technique following the National Security Agency highly mediatized issue of calls and e-mails registration. What is important though is to also use a proper awareness procedure for the commonly understanding of population regarding their need of protection on their own benefit. In this case, similar with the monitoring of digital networks for cyber viruses, the gain is higher than the price paid.

Also, in the medical field the situation is even more sensitive, because of the patient's rights. Special procedures have to be put in place for a proper communication and report of diseases. Often, statistics are not enough for the prediction of epidemics so the infected persons and their medical file has to be analysed or transmitted transnationally.

In this respect, common people often misunderstand democracy and human rights. Someone's rights and liberties do not have to surpass another's rights and liberties. Unfortunately, in a highly interconnected world, as the world we live in, is very difficult to establish proper boundaries and often limitations are easy to be broken. Emerging threats, due to their asymmetry, bring forward this need of monitoring their specific elements, for the common good of populations and societies.

An Early Warning Intelligence system could be created, in order to systematically collect, analyse, interpret and disseminate data. This system could function similarly for effective infectious disease control and for cyber attacks surveillance.

Collectors of intelligence on these types of transnational threats increasingly have to do their own, on-the-spot analysis in order to validate information and prioritise collection targets against a rapidly-evolving threat.

These transnational issues, because of their induced high degree of interdependence between states, are also challenging traditional intelligence structures, blurring the distinction between domestic and international intelligence collection as well as that between the public/state sphere and the private/societal sphere of security.[17]

On the other hand, sharing of intelligence and tradecraft raise concerns about the protection of sources and methods and the impact on future counter-intelligence capabilities. Expanded intelligence liaison brings also a greater amount of intelligence material of uncertain reliability for intelligence analysis organisations, which acts as a perturbing factor in achieving an accurate analysis of intelligence indicators.[18]

Beside the issue of state sovereignty, often remembered in the intelligence sharing discussions, the problems brought by cyber-attacks is challenging the intelligence network – as DoS or information leakage, and make the intelligence agencies more reluctant to cooperation.

For all these reasons, intelligence sharing approach should become more comprehensive and should be conducted on appropriate frameworks for each specific threat, turning more flexible and adaptable to the technological changes. A transformed Intelligence Community with strategic capabilities is needed, equipped to develop long-term plans for the new security threats and to identify social trends shaping the future threats. Lastly, in the process of enhancing intelligence sharing on specific issues, such as epidemics outbreak or cyber attacks, one has to remember that no matter how well-structured an early-warning system, its success depends, above all, on the judgment and vision of political authorities. Ultimately, it goes to show the political will to act collectively when transnational threats tend to affect the collective security.

References

1. Costin Cernescu, Simona Ruţă, *Progrese în controlul şi prevenirea virozelor cu potențial bioterorist,* (Bucharest: Ed. Universitară, Carol Davila, 2004), p. 1.
2. Costin Cernescu, Simona Ruţă, *op. cit.,* p. 1.
3. Phil Williams, "Intelligence Requirements for Transnational Threats: New Ways of Thinking, Alternative Methods of Analysis, and Innovative Organizational Structures", *New Frontiers of Intelligence Analysis,* (Rome: Global Futures Partnership of the Sherman Kent School for Intelligence Analysis and University of Malta, 2004), pp. 49.
4. *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, http://www.opbw.org/convention/conv.html*
5. http://www.who.int - 4
6. http://www.who.int/csr/alertresponse/epidemicintelligence/en/index.html - 5
7. http://www.ecdc.europa.eu - 6
8. http://ec.europa.eu/health-eu/newsletter/113/focus_newsletter_en.htm - 7
9. http://ec.europa.eu/enterprise/newsroom/cf/Securing-public-events-against-terrorist-attacks-and-other-threats-via-the-innovative-integration-of-diverse-technologies
10. http://medusa.jrc.it/medisys/homeedition/ro/home.html - 9
11. http://www.cert.europa.eu - 10
12. http://www.us-cert.gov/ncas/bulletins
13. http://www.enisa.europa.eu - 12
14. William Jackson, *Best defense against hackers: Know your enemy,* GCN, 2010, http://gcn.com/articles/2010/06/28/cybereye-know-your-enemy.aspx - 13

15. G. Eysenbach „Infodemiology and infoveillance: framework for an emerging set of public health informatics methods to analyze search, communication and publication behavior on the Internet", *J Med Internet Res* 11:e11, 2009.
16. http://www.who.int/flunet
17. Salathé M, Bengtsson L, Bodnar TJ, Brewer DD, Brownstein JS, et al., „Digital Epidemiology", *PLoS Comput Biol* 8(7): e1002616, 2012, http://www.ploscompbiol.org
18. Gregory F. Treverton, "Reshaping Intelligence to Share with 'Ourselves," *CSIS Commentary*, No. 82, Summer 2003, pp. 5.
19. Michael Wesley, „Analysing Transnational Intelligence", *New Frontiers of Intelligence Analysis*, (Rome: Global Futures Partnership of the Sherman Kent School for Intelligence Analysis and University of Malta, 2004), pp. 100.

Intelligence Products as Tools for Decision Makers in the Management of Environmental Crime by Law Enforcement Institutions – The Case of National Environmental Guard

Francisc TOBĂ[*]

Abstract

The problem of the management of environmental crime (ecological crime/eco-crime) will be one of the most important issues in the field of national security. To manage in the proper way this challenge is more and more important, for all law enforcement agencies in the environment field, to have the full support of the products of intelligence.

The eco-crime is one of the problem of the organized crime and transnational activities that would affect the stability of the nations to manage for sustainable development the natural resources and to preserve the national environment security.

To use in the proper manner the intelligence products means to have one very good network which include the intelligence agencies and national law enforcement agencies, like national environment guard, based on high speed exchange of the intelligence products and proper early warning system. At the end of the entire process we need to build a good justice system to protect the right of the people to have a national health environment.

Keywords: national security, environmental security, wildlife crime, trans-border criminality, organized crime

Premises approach

Opening the intelligence community – namely the National Intelligence Academy in the Romanian Intelligence Service – joining efforts on knowledge and performance of the management of national and international environmental variables of the current security and by appealing to the development of security studies show interest and responsibility on the potential national academic. Appeal on the points of view characterized by diversity and innovation outside the intelligence community provide to the institutions involved in implementing intelligence waypoints idea that national security issues is not exclusive monopoly of the state.

[*] Assistant Professor Ph.D., "Spiru Haret" University, Romania

The volatility of the current security environment determines the emergence of new paradigms, with "variable geometry" and requires the identification, development and implementation of models characterized by adaptability to the new family of vulnerabilities, risks, threats and aggressions. From the perspective of proactive social processuality of the specific human civilization of the new millennium's the role of intelligence becomes crucial (human factor becomes the driving wheel of this approach) and enhances holistic approach by "coupling" several actors onto specific processuality of the national intelligence authorities.

Sliding the modes of aggression towards non-military sphere has brought to the fore more refined forms of threats, most often undetectable by conventional early warning systems. From this perspective the economic attacks (see the battle for natural resources vital for the carbon-based economy or for the global monopoly segments of the market), financial banking, imagological, cultural, religious or environmental aggressions become the "nuclear" vectors of the new millennium.

The natural environment has become "theater" of global-scale operations. Economic war or the resource curse has become common phrases of the current language. Gunpowder was replaced by decisive gas valve. As Robert Service said "Russia remains dangerously dependent on global prices of oil, natural gas, diamonds and timber, with still a need to diversify the economy." Adapting to the new demands of globalization surprises and concerns in equal measure, the state's population as well as the international community.

A case in point is Canada. As Andrew Nikiforuk argues "In the last decade, Canada has become, in silence, a center of international mining and a lawless petrostate". And significant advocate, for the theme of our work, that the federal government "shut the scientists talking about climate change, killed funding of any kind for environmental sciences, and through a recent pair of laws abolished unprecedented and systematically the most significant and most respected environmental laws of the country" . Because the reality is very clear to all, the author argues that a secret document of foreign policy came in the fall of 2012 at the Canadian Broadcasting Co., the new administration proposes new priorities: "To succeed, we must seek political relations tandem with economic interests and where political interests or values may not align." Canadian model seems not singular and the developments in the exploitation of natural resources in Romania supporting national public concern.

Ambassador George Cristian Maior, director of the Romanian Intelligence Service, noted that "the challenges of the beginning of the millennium are multiple, from the valences, not yet fully understood, of globalization until the perverse facets of new threats for states and individuals such as terrorism or ecological changes ". Worthy of note is the idea that the director of the Romanian Intelligence Service placed at the same level: terrorism with ecological changes in global threats palette!

On 14th October 2009, at the initiative of the Alliance Professionals for Progress (APP) held in Aula Magna of Romanian Academy public debate on "State Reform", the first reunion from the cycle "After the crisis - where?". The participants decided to send a letter to the Romanian Government were several ideas, such as: "The fundamental question to be answered is whether, after the crisis, Romania will continue to follow the same path of growth based on *irrational use of resources* with low added value and emphasizing social inequalities or will be able to take away new European model of sustainable development by organic combining the social and economic aspects with the environment aspects."(s.n.). The letter indicates the need for introduction under the general indicator of GDP - growth GDP of the complementary indicators, reflecting the qualitative, social inclusion, preserving a healthy natural environment, rational use of resources in terms of eco-efficiency and the best use of human resources.

Climate changes are evolving mega processes with another time scale in relation to what the consumerist civilization understood as temporal reference system. The globalizations of economic processes have led inter-planetary, within the fewer are the beneficiaries of the profit, and more and more are destroyed by natural disasters. Nature imposes more severe rethinking human relationships with nature, the urgent need to move from the civilization of profit towards a resource-based civilization.

Environmental security enables awareness of the limits of these ratios and appropriate ways to reduce imbalances and redirecting human activity to cooperation and not confrontation with incorporating environment. Activities of "therapy" like restoring natural affected ecosystems or recycling should be accompanied by activities of "prevention" preventive, predictive and minimizing the adverse consequences of human activities on the surrounding environment.

The partnership between man and nature is the only win-win solution and represents the only option if the human race wants to exist on Earth. Environmental Security considers both bios security as well as how the natural resources as a result of human activity, supporting the existence of the bios. The development of human civilization must not weaken the surrounding environment.

The Ecuadorian Constitution of 2008 expressly provides: Nature or Mother Nature where life is reproduced and exists, has the right to exist, persist, maintain and regenerate vital cycles, structure, functions and its evolutionary processes. It also states that every person, community and nation must admit recognizing the rights of nature to the public institutions.

Since 1972 the government of Bhutan has replaced the indicator "gross national product" with "gross national satisfaction" and allocated significant funds for educating citizens in a spirit of happiness, sustainability, justice and peace. The first objective of this exceptional indicator is the integration of human interdependence with nature and achieves a permanent system which combines personal psychology variety of cultural and ecological system.

The issue of the management of resources and especially access and exploitation of sustainable development is increasingly becoming an issue of national security management, is being clearly included in what we define to be *resources of security*. Former Secretary of State Colin Powell says (2002)[1] that sustainable development is a matter of morality and humanitarianism simultaneously, but at the same time it is a *security imperative*. Poverty, *environmental degradation* and despair of the individuals and the entire human communities are destructive factors of societies and nations and the aggregation of these factors can destabilize countries and even entire regions. (s.n.)

Environmental security or ecological security becomes obviously one of national priorities systems and international safety management. From this perspective, environmental crime manifests itself in ways more subtle and more harmful. The international community is fully aware of this threat, trying to redraw the environmental legal framework as well, especially institutional reconfiguration – international and national – to allow proper management of this phenomenon.

One of the most important levers is the collaboration between law enforcement institutions and those that can provide relevant information on environmental crime. In Romania the only institution empowered to valorize information on environmental crime as an institution designed to enforce environmental legislation is the National Environmental Guard. In our documentation we requested – both the National Environmental Guard as well as institutions in the sphere of intelligence, the Romanian Intelligence Service, or DGIPI Romanian Foreign Intelligence Service – their viewpoints on the present theme. In this way we wish to thank the institutions that were willing to support our efforts documentation.

International context

Crime and other illicit activities against the environment are currently one of the most profitable forms of illegal business. They are one significant threat pose a security and safety for more and more countries and have significant negative impact on sustainable development and the rule of law.

Interpol – International Crime Police Organizations – estimates that global wildlife crime is worth billions of dollars a year. The economic value of global illegal logging, including processing, is estimates to be worth between 30 - 100 billion USD, approximately (10% - 30%) of global timber trade.

INTERPOL

Formed in 1992, the E*nvironmental Crime Committee* assisted Interpol in identifying emerging patterns and trends of environmental crime enforcement.[2]

During the INTERPOL/UNEP International Chiefs of Environmental Compliance and Enforcement Summit in March 2012, the decision was made to restructure the Environmental Crime Committee with new identity *Environmental Compliance and Enforcement Committee (ECEC)* which put together executive leaders and decision makers from member countries of UNEP governing council to provide advice on relevant issues and to hornet global impact. The 1st Meeting of the Environmental Compliance and Enforcement Committee was hold from 6th to 8th November 2013 in Nairobi, Kenya, alongside meetings of *Wildlife, Pollution and Fisheries Crime Working Groups* from 4 to 7 November 2013.

Environmental crime is a serious international problem and or most importance. This threat to the national and international security takes many different aspects and broadly speaking, wildlife crime is defined as the illegal exploitation of world's flora and fauna and pollution crime is the illegal trading and disposal of hazardous waste or resources.[3]

Today and in the future new types of environmental crime are emerging, such as carbon trade, water management crime or climatical aggressions.

Organized criminal network is trans-border and can affect a nation is economy, security and even its existence. Most of the wildlife or pollution crime is carried out by organized criminal network, because these types of activities are characterized by the low risk and high profit.

To manage this type of crime in proper way there is need for an international strategy and INTERPOL is the only organization with mandate to share and process criminal information globally. The Interpol Crime Program (EPC) leads global and local operations to neutralize and dismantle the criminal networks behind environmental crime using *intelligence-driven policies*, coordinates and develops international law enforcement best practice manuals, guides and other resources.

The INTERPOL ECP sustains environmental law enforcement agencies with access to these services by enhancing links with INTERPOL National Central Bureaus. In this respect it was promoted *Interpol Ecomessage*[4] Intelligence-led policing which is emerging among INTERPOL members as a new and targeted approach to environmental crime.

Within this model, sensitive information is collected, recorded, evaluated and also researched via INTERPOL's unique resources. Using those intelligence products both INTERPOL and national decision-makers can proactively identify high-risk areas and persons/organizations and to promote the right operations. The INTERPOL Ecomessage system provides uniform intelligence products for many different law enforcement agencies, both at national and international level. Those agencies are not necessarily a police agency but, often a designated authority with investigation powers, such as *environmental inspectorates* and wildlife authorities. In Romania the National Environmental Guard manages this type of investigations.

UNEP[5]

In November took place *Interpol-UNEP International Environmental Compliance and Enforcement Conference*[6] where high-level national enforcement officials, and ministerial/ government representatives, were present relevant organizations and representatives from civil society which will work together in this unique forum to debate various aspects from environmental tendencies to the impact of violations of environmental law.

They will discuss about realistic solutions and the impact of new and existing tools in combating these processes and reach an agreement regarding the action points for the near future.

The working groups and the discussions within the Conference will responde to the challenges in law enforcement like:

1. Barriers of engagement
2. Overcoming the obstacles and building capacity
3. Managing a changing financial environment
4. Effective enforcement networks and regional engagement.

The discussions will be led by separate convening panels concerning the four themes:

1. *Intelligence and information management*
2. Investigation and operational support
3. Capacity building
4. International strategy

The Conference developed a global strategy and enhanced a state of efficiency and effectiveness, utilizing the existing expertise and skills in the world. The approach of the Conference will be based on considering the evidence of current and emerging threats and the role of strategical and tactical analysis at the national, regional and international level. The debates will identify key priorities and the path forward regional and international responses to environmental, biodiversity and natural resources security.

The INTERPOL-UNEP Conference, on 6th November 2013, brought together executive leaders from around the world to design an international joint strategy to manage environmental crime. Cooperation between intergovernmental organizations, as well as the environmental enforcement actions of focus for the international community in the next years, were the main topics of discussion during the conference. INNTERPOL and UNEP recognize that only by working together, within common objectives and strategies will truly have a major impact on the activities of the individuals, networks and companies that illegally exploit global environment, biodiversity and natural resources.

United Kingdom

In United Kingdom exists a specific authority dedicated to manage the problem of environmental crime *National Wildlife Crime Unit*[7]. The people can call to 999 in case of considered actions which can be one environmental crime or call the police office. The structure of NWCU includes: one head of office, senior intelligence officer, senior analyst, investigative support officers (3), intelligence officers (1 full-time, 2 part-time), internet intelligence officer, indexer and analyst.

Investigative Support Officers offer free assistance to police forces and partners across the whole of the United Kingdom. The slogan of NWCU is *"combating wild crime by communication, cooperation and coordination"*.

Environmental Task Force[8] was put in place to manage in the proper way the most important issue of environmental crime. It was created after the Summit (Edinburgh, November 2011) and it will be well equipped and fully dedicated to manage the problem of environmental crime. The Summit made some very important suggestions concerning the right actions in this sense, like:

1. to adapt the legislation in the environment field – to simplify the identity of targets and to be more efficient;

2. to develop the collaboration and the dissemination of intelligence between the agencies of law enforcement and to improve the punishment process;

3. to develop one more clear set of punishment in this field.

The activity of ETF will be based on more efficient process of gathering intelligence and more effective dissemination process which will improve the performance of this task force.

National context

In Romania the institution with responsibilities in the field of taxation law in the environmental field is the National Environmental Guard (NEG), under the coordination of the Ministry of Environment and Climate Change. At the beginning of 2014, National Environmental Guard operates under the Government Decision no. 544 of 30 July 2013, which changed the Government Decisions no.1005 from 2012 on the organization and functioning of National Environmental Guard.

NEG is a specialized institution of the state in the sphere of control and inspection in the environment field, reflecting the application of government policy in the field of prevention, ascertaining and sanctioning violations of the law on environmental protection and play an active role to ensure the environmental security through actions of risk prevention and limiting ecological threats.

In compliance with article 4 of the Government Decision No. 1005/2012, NEG cooperates in this regard with the state authorities and public institutions, central and local public administration, representatives of civil society with legal and/or physical persons, with institutions with similar duties in other states based on international treaties to which Romania is a party or signed protocols on a reciprocal basis and with international organizations of public and/or private sector within the European Union in cases of common interest or within the international project or programmes.

Given that NEG has expressed powers in the environmental security, which is part of the national/European security - with military security, political security, economic security, social security, we consider that this institution should be considered as part of the national security system.

NEG has made a significant set of protocols with core institutions of the national security system: the Ministry of Defense, Ministry of Interior (Gendarmerie, Interpol, Customs, DGIPI) and Intelligence Service. Based on the information provided by these institutions, the action of the Commissioners/ Inspectors of NEG increased in efficiency. Environmental crime has become a reality and it cannot be managed only through cooperation and harnessing the potential of all institutions empowered to action in this area.

National Environmental Guard has received over 250 informations from various institutions in the sphere of national security, during 2013. In this regard, for example, DGIPI provided analytical products as follows: 75 (2010), 42 (2011), 41 (2012) and 15 (2013). In the DGIPI there is a database in which is stored including information on environmental risks. At the institutional level there are quarterly analyses on environment crime in order to maximize the exploitation of informations and effective management of vulnerabilities and threats on environmental security.

In the framework of collaboration between the National Environmental Guard and the Romanian Intelligence Service (RIS) information flow is not unequivocally, due to the fact that the beneficiaries of this information have the opportunity to apply to RIS to provide data of their field of responsibility, completion and further explanation. The Romanian Intelligence Service has maintained a high availability on the identification and adoption of institutional mechanisms that favor exhaustive coverage of topics of interest to national security, including from the perspective of entitled beneficiary, according to the principle of "need to know".

Conclusions

National and international security becomes an increasingly complex area and as such is required auto-adaptive institutional models, both through cooperation and through interdisciplinary and trans-institutional approaches. The Third Millennium brings forward the human existence the new dimensions of global security, such as cyber security, cultural security and the human security.

Managing these new challenges can be achieved only through a coherent and consistent legal and institutional framework adapted to the socio-economic evolution. Institutional communication and capitalization in real time as potential action of each institution is the only chance to manage crime in the sphere of environmental performance.

Institutions involved in intelligence community must become decisive decision support - by providing intelligence products performance - for law enforcement institutions, regardless of the reference field.

From our perspective required several courses of action, as follows:

- adapting the legal framework on the environment sphere both in scope as well as the sanctioning actions that are within the scope of environmental crime;
- development of specialized courts in the Ministry of Justice;
- National Environmental Guard shall develop a minimum potential, allocation of specialized human resources, information and analysis to realize a database enabling strategies for effective action.

Countering environmental crime can only be achieved by resorting to law enforcement performing institutions and consistently involving the intelligence community, together with the development of suitable justice architecture to the new ways of breaking the law.

References

[1] http://www.un.org/jsummit/html/media_info/pressreleases_factsheets/unep_ press_release_508.pdf

[2] http://www.interpol.int/Crime-areas/Environmental-crime/Environmental-Compliance-and-Enforcement-Committee

[3] http://www.interpol.int/Crime-areas/Environmental-crime/Environmental-Crime

[4] http://www.interpol.int/Crime-areas/Environmental-crime/Ecomessage

[5] UNEP – United Nations Environment Program

[6] Draft timetable of Events 4-8 November, 2013, version 160913.pdf

[7] http://www.nwcu.police.uk

[8] http://www.scotland.gov.uk

Terrorist Have Just *Signed in* on Facebook – An Analysis of the Ways in Which Terrorist Use Social Media –

Raluca LUȚAI[*]

Abstract

In the XXIst century social networks such as Facebook or Twitter are an important part of every modern individual. In these conditions the intelligence community is facing a great challenge and the role of Open Source Intelligence is becomes crucial. Always careful and innovative the terrorist networks saw the great potential of these social networks and started to use them in spreading their message and recruit new adherents. They are using it so much that Facebook and Twitter is now a perfect environment for achieving soft power.

This paper is a qualitative and subjective analysis of several Facebook pages used to spread extremist ideologies. Our analysis starts from the assumption that the social network created by Mark Zuckerberg can be a useful recruitment and mobilization platform for terrorists. In this sense our main objective is to demonstrate that Facebook is and can be a efficient tool in spreading radical messages.

In the attempt to prove this hypothesis we will follow several pages and profiles and we will take a closer look to the pictures, videos or statuses posted in this pages. The pages and the profiles we will look at will be selected by searching some keywords like Osama bin Laden, Jihad, Islam, or Mujahedeen and for analyzing the posts and the pictures we will use the content analysis method.

Keywords: Facebook, terrorism, social media, radicalization.

Introduction

In a century of innovation and development the new technologies are available for everybody. The Internet is the brand new place for communication and expression. Social networks like Twitter, Facebook or MySpace are offering a free and unconditional medium for expression and because of this they are an important part in everybody's life. Starting from this assumption we can not overlook the importance of this social networks for radical groups or terrorists.

The central idea behind the present approach, is the fact that as well as anyone else the terrorists are using the internet in their

[*] MA Student at National Intelligence Academy, Romania

attempt to conquer the world. Taking advantage of all the benefits offered by the Internet they manage to transform it into a propaganda and radicalization tool.

This paper is a qualitative and subjective research of Facebook and the ways in which radical groups use to it to spread their radical message. Following a number of indicators such as: images, videos and text messages they post, we analyzed a number of eight pages administrated by people or organization with radical views.

Without any claim of completeness, our approach started from a theoretically framework in which we outlined some theoretical elements useful in our research. The discussions are the result of an analysis process of some Facebook pages and the conclusions that we reached affirms the hypothesis form which we started.

Theoretical background

Developed by the end of the last century, the Internet has become nowadays one of the most important means of mass communication. As part and premise of the globalization process, the Internet has become an important aspect of everybody's life and also in the life of states or organizations. This new step is more than normal in a globalized society where connections are formed between people, businesses, institutions located thousands miles away.

Information and technology advancements have always been those who have driven the development trend in the intelligence field[1]. It is beyond any doubt that this new flow of information coming from the Internet will have a great impact in the intelligence community in general and it will affect some issues in particular.

Terrorist groups, in their permanent process of adapting strategies towards achieving their goals have glimpsed the benefits offered by the internet. It is said that terrorism is a particularly negative and morbid form of communication. In this context we can easily say that the terrorists are using the internet just like everybody else[2] in their communication process. The brand new attraction for they is represented by the social networks. This is confirmed by studies and data which considers that approximately 90% of terrorist activity on the Internet is focused on social media[3]. Networks like

Facebook, Twitter and MySpace provide a framework for the events of each of us, and functions as a cluster[4] in which the individual gets easier access to other individual information.

Facebook is now the most successful example of social networks. Launched in 2004 as a communication platform between several American universities, Facebook has grown and transformed itself in the global phenomenon of this decade. With no less than 1.15 billion users[5], the network aims to give people the power to share, and make the world more open and connected[6]. Data show that approximately 222 million users join annually the network, 66% of whom are from the Middle East and 23% in Asia[7].

Most of those who are members of this network are using it as a communication space, as a place for information and for linking connections with individuals who share the same ideas, but also for relaxation purposes. For terrorists, social networks are the most attractive and at the same time challenging "playgrounds". Noting that it has influence on the lives of individuals who use it, the terrorists have built on Facebook a battle front that operates in several directions. We believe that the use of social media sites like Facebook is a natural progression of their technology oriented tactics.

The benefits that a social network offers you are undeniable and the terrorist "invasion" of them is almost obvious. Social networks like Facebook safeguards the identities so that everyone can create their own virtual *me*. Terrorists will not choose to use their own names but will hide behind symbols of religious or ideological nature. In this case Facebook fosters an environment in which individuals can be senders and receivers of a certain message without fearing anything.

Talking about messages, Facebook is an ideal medium for propaganda, a perfect jihadist media device[8] and a non ideological medium which allows them to reach a wider audience. Terrorists have learned to enjoy the multimedia environment provided by Facebook to spread the message, to carry out the objectives and for the online exchange of guidance, advice and instructions. The instantaneous update capabilities are helping them to organize more precise ambushes. Besides this, Facebook allows them to monitor individuals and to collect dates about a certain target group. In this way Facebook works as a real-time intelligence source and platform for collecting information. Facebook is a medium through which terrorists succeed to built connections between its members, protecting itself from the enemies while the ultimate goal is to indoctrinate and radicalize people so they feel compelled to commit acts of terrorism for them and their cause[9]. In this sense terrorists will use Facebook to target millions of young users and disseminate audio video and textual jihadist literature.

In a report by the Department of Homeland Security "Terrorists use of social networking sites: Facebook Case Study" authorities include how terrorist groups can use their Facebook network in their favor. The authorities concern comes from the fact the terrorist can: share operational and tactical information, including bomb recipes and weapons maintenance or use Facebook as a medium of propaganda: *In this way, Facebook acts as a gate away or laundring pad for further radicalization and for easy access to sites where explosives recipes and IED information are regularly posted.*[10]

Facebook ”Invasion”[11] is the second stage in terrorist actions to conquer the Internet after the first phase of the invasion that had targeted the You Tube website. Aware of the importance of social networking, a user of the forum jihad is tal-Faloja encourage other members to increase their Facebook activity arguing that *If american politicians like Barack Obama can use it to win an election, we can use it to take over the world*[12]. Another user of a jihadist forum quoted in the Department of Homeland Security report affirms the following: *I entreat you, by God, to begin registering to Facebook as soon as you finish reading this post. Familiarize yourself with it. This post is a seed and a beginning to be followed by serious efforts to optimize our Facebook usage. Let’s start distributing Islamic jihadi publications, posts, articles and pictures. Let’s anticipate a reward from the Lord of the Heavens, dedicate our purpose to God and help our colleagues*[13]. We see how useful is for terrorists to send their message on Facebook and how much it encourages jihadist activity in this social network.

Being a *mise on scene* of open source intelligence, an environment in which information flows in real time, some terrorists are convinced that any kind of manifestation on Facebook can turn against them. Aware of this, a user of a jihadist group warns his colleagues about the following threats: *Don't make a network on Facebook...Then kuffar will know every friend you have or had in the past. They will know location, how you look, what you like, they will know everything! Join Facebook if you want and use it to keep in touch with friends and brothers from away but not as a network*[14].

The Internet has long been a favorite tool for terrorists but in the context of the growing importance of social networks it becomes an important front against the infidels. New media and social networks interconnect so much individuals as the so-called *dumb mobs* made up of ordinary individual scan be transformed into *smart mobs*[15] of active person ages who are linked by notebook computers and who are willing to commit or engage in terrorist acts. As part of this new media revolution, Facebook and its interactive capabilities like chat rooms, the sharing possibilities and the online communities allow terrorists to assume an offensive position.

Aims and objectives

Starting from the assumption that new media through social networks are a new battle front for terrorist groups, this paper seeks to demonstrate that the network created and developed by Mark Zuckerberg in February 2004 is a perfect environment for terrorists who want to spread their message and to mobilize supporters.

The main objective of this paper is to demonstrate the usefulness of the Facebook network in the architecture of the terrorist networks, namely, in the spread of radical messages.

Tools and methodology

From the methodological point of view, our approach is built on a qualitative and subjective analysis conducted through document analysis. Ideas and conclusions that will be discussed in the next section are the result of scanning of eight Facebook pages through some indicators.

The grid analysis that we intend to use it in the direction of demonstrating the utility network Facebook in spreading radical messages comprises three dimensions. The eight pages of Facebook will be analyzed in terms of **images** (men, women, children, abstract/religious materials) the **register** (informational / religious / inspirational-instigator) in which are the statuses written and **videos** (religious / motivational / informational war-related issues) posted by users. We consider that these indicators are the most suggestive for the approach that we initiated because the pictures, videos and messages are useful means of communication between users and receives.

These eight pages of Facebook that will be filtered by the indicators listed above were selected through the Facebook search engine. Keywords for searches that were made are: *jihad, mujahedeen, Islam, terrorism*.

Results and discussion

The analysis of the eight pages of Facebook reveals that radical groups are present on the social network. The eight pages that we analyzed for videos, pictures and statuses they cover are clear examples of how terrorist groups can use online media to spread messages and attract new members.

Regarding the videos that they promote, we noticed that they are often full of violence. They feature either mujahedeen who are preparing to fight, or the damaging effects of the attacks that they manage to realize. Another category of videos posted on Facebook are those that include motivational messages of leaders, be they local or of great leaders. Motivational videos are made either inside or outside and are always accompanied by a specific soundtrack. The videos are an important mean of propaganda and an extremely important attraction because they manage to bring together in a few minutes material both picture and sound. If the message they convey is accompanied by the ideal image and a soundtrack that will attract attention than their success is undeniable. Administrators who are behind the pages were viewed selected very careful and suggestive videos in the direction of propagation of their ideas and objectives.

Like the videos the pictures and images present on the pages that we study can be an indicator of the utility of this social network. Analyzed Facebook pages abound in images that are appreciated, sometimes by a large number of users. The analysis that we performed allowed us to reach some conclusions concerning the categories of pictures promoted on this pages. Thus, we concluded that the images can be summarized into four categories:

- The man image
- The women image
- The child/baby image
- Other images.

The man is the most frequent character on the photos of these social pages. Men are often presented as soldiers, servants of Allah, ready to fight against the infidels. Individual and group pictures of soldiers of Allah are a leitmotiv of each page examined. Besides the common soldier's the Facebook pages popularize images of the great leaders. Photos of Osama bin Laden, the current leader of the Al Qaeda-Al Zawahiri or other leaders are also present. Pages albums include among other martyrs who have sacrificed their lives for the idea organizations, martyrs who should be praised and an example for everyone.

Women hardly present in the analyzed page images are an example for the Muslim community. They are captured in two different hypostases. The first is the woman who, like her man, is preparing for battle. Plenty of pictures on the analyzed pages are showing the women training or their "battalions" of soldiers ready to fight for their cause. The second stance portrays women as injured victims, victims of the damage caused by the enemies. This stance must be a mobilizing factor for their lover husbands, husbands who even though they don’t have a great respect for them, should not allow this kind of situations, and must fight against those who produce such things. Images like these are used to generate violent behavior.

The child is also an important element of this pages. Page administrators are aware that emotion sells and often use images of children or adolescents in the desire to generate radical cognitions and behaviors. Children killed or injured in the attacks are a constant and important motivation for those who serve Allah. On the other hand, children are often portrayed as future terrorists. Often photographed next to weapons, fighting or training for it, children are used as an example for adults.

Other common images on this pages include anti-Israeli messages, motivational images, are showing the victims of attacks, different religious teachings and spread various causes, such as of Syria. The flag of Jihad so well known and popularized by Al Qaeda is also present in on almost every page of Facebook analyzed.

Thus we see that the images promoted on Facebook rely on the fact that they will born or will justify certain behaviors that are consistent with organizational objectives.

Regarding the messages promoted as statuses on the 8 pages, we conclude that these belong to three broad categories: religious, threatening or of a motivational/instigator nature.

In the category of religious the users urge those who visit the pages to follow Allah, to follow the rules recorded in the Koran and pray for those who struggle against the infidels.

Among the most representative inflammatory messages that I have encountered are:

”so revenge dog, revenge”

”take a gun and fight against (the enemy)-only one solution Jihad”

”the most beautiful death in life is the death under the banner of Jihad”

”the victory comes from loyalty and followers”

Threatening:

”our brothers and sisters died, but our relation die never we're ready for Jihad against kuffar.. we're ready for giving blood..insha Allah”

”humiliation could not bring invitation and peaceful coexistence conferences! But raising the trigger”

This message accompanied by suggestive images and videos make Facebook a more than favorable radical messages.

Conclusions

The Internet has always been an important tool for the terrorists but with the growth of social networking it becomes more and more important, a front against unbelievers. New media and social networking connects individuals so much that they can take part of a radicalization process orchestrated by terrorist and their pages.

As part of the new media revolution and due to its innovative capabilities like chat rooms plus various opportunities to share information, Facebook is a place that offers terrorists an offensive position in their relationship with the world. As we saw during our research, terrorists use this network to spread their radical message or for the recruitment of new followers. Through the videos, the pictures they spread they manage to justify or to produce violent behavior and by the messages they spread they manage to spread their ideology.

Because of its capabilities, Facebook can be a new playground, a new front in the fight against the infidels. For the intelligence community, social networks as Facebook can be a challenge and an opportunity in the global fight against terrorism.

Limitations

The present research encountered several obstacles that influenced the analysis. The rapidity with which any process is carried out in the online environment has given us trouble sometimes because the Facebook pages that we analyzed were sometimes updated too fast. We also met the situation in which pages were abolished. This can be an indicator of the content of such pages is the virtual environment.

On the other hand, we have dealt with various language barriers. Many of the selected pages were written in languages such as Arabic, Malaysian or Urdu. This forced us to use Google Translate engine for the translation and perhaps sometimes the message have lost accuracy.

References

[1] Dragoş Dinu, Maria Daniela Bunoiu, ”Impactul evolutiilor tehnologice asupra OSINT” in *Revista română de studii de intelligence*, nr. 4, december 2010, Bucureşti, p. 57.

[2] Maura Conway, *Terrorism and the internet. New Media-new threat?* Available at http://doras.dcu.ie/515/1/parliamentary_affairs_59_2.pdf , p. 1

[3] Grabriel Weiman, ”Terrorists Facebook: terrorists and online social networking”, in *Web Intelligence and Security: Advances in data and text mining techinques*, (ISO Press,2010), p. 19.

[4] Acording to the ”small world ” theory by D. J. Watts in Social Network Analyisis as an Aproach to Combat Terrorism. Past, present and future research”, in *Homeland Security Affairs*, vol. 2, 2006, p. 2.

[5] Data form March 2013, according to http://investor.fb.com/releasedetail.cfm?ReleaseID=761090, accessed in 30 August 2013.

[6] https://www.facebook.com/facebook/info, accessed in 30 August 2013.

[7] Gabriel Weiman, *Al Qaeda has sent you a friend request: terrorist using online social networking, (*Israeli Communication Association, 2011), p. 7.

[8] *Idem*, ”Terrorists Facebook: terrorists and online social networking”, in *Web Intelligence and Security: Advances in data and text mining techniques*, ISO Press, 2010, p. 6.

[9] Todd Waskiewicz, *Friend of a friend influence in terrorists social networks*, available at http://world-comp.org/p2012/ICA6143.pdfp.1 (accessed in 27 august 2013).

[10] Jana Winter, *Al Qaeda looks to make new friends on Facebook*, available at: http://www.foxnews.com/tech/2010/12/09/facebook-friends-terror/, accessed in 2 September 2013.

[11] Gabriel Weiman, *op. cit.*, p. 26.

[12] *Al Qaeda plans to wage holy war on Facebook*, available at http://www.telegraph.co.uk/news/worldnews/3885367/Al-Qaeda-plans-to-wage-holy-war-on-Facebook.html,accesed in 2 September 2013.

[13] Yael Stein, ”Social Networks-terrorism s new market place” in *Genocide Prevention Now*, vol. 1., 2010, p. 3.

[14] Grabriel Weiman, *Al Qaeda has sent you a friend request: terrorist using online social networking, (*Israeli Communication Association, 2011), p. 7.

[15] The dumb mob vs. smart mob theory is written by Howard Rheingold (2002) and described in the paper of Richard Kahn, Douglas Kellener, *New media and internet: from the battle to settle to blogging, in New Media and Society*, (Sage Publications, March 2009).

Understanding the Power of "Multitudes". Detecting Factors of Change in Collectively Created Spontaneous Narratives Online

Cristina IVAN [*]

Abstract

*The paper addresses the overtheorised and underspecified concept of multitudes (Hardt&Negri: 2004)***.** *Aiming to provide new insights into how this concept can be detected in emerging patterns of social action in the online environment, it advances with a detailed analysis of social networking configurations of heterotopic space and offers a personal view on the social functions of hyperreality at the beginning of the 21st century. It continues with a detailed case study of the narratives provided in a recent Romanian protest movement, called Save Rosia Montana, sparked and glued on the social networking site Facebook. The paper ultimately argues that social networking sites create a hybrid illusion/reality of space in the non-place continuum of our contemporary world, thus allowing individual and collective agency to emplace desires and ideals of home, patriotism, freedom, purity. It is the author's intention to demonstrate that a new paradigm of thought beyond post(post)modernism is currently emerging and by understanding it, we can prepare ourselves to detect factors of change.*

Keywords: multitudes, social networks, participatory democracy, save Rosia Montana, change, social activism

Introduction

Some 20 years ago, in a journalistic triptych published in the French newspaper *Liberation*[1], Jean Baudrillard daringly announced the victory of hyper-reality upon our lives. His articles questioned the idea of live journalistic coverage of war events. He drew attention to media strategies employed to create simulated *versions* of reality that kept audience away from real facts by creating the visual simulacra of a technologized, videogame-like narrative of war that deleted carnage, victims and death and promoted a "clean" targeting of abstracted victims, in tune with the rhetoric of the state. As Peter Childs notes in a comprehensive, in-depth analysis of Baudrillard's texts[2], what Baudrillard attracted attention to was **the advent of a new paradigmatic approach, based on the suppression of the real and imposition of the virtual**. The conclusion was rather gloomy, **predicting an epoch in which technological choreography was about to wipe off direct interaction with events and lead to the creation of entirely mediated and therefore manipulated perceptions on the part of the public[3].**

[*] Researcher, The National Institute for Intelligence Studies, Romania

This has lead, as we know, to a whole line of criticism announcing a doom-like reality being created into the 21st century, one in which alienation and isolation were to become viral, affecting behavior of citizens across the world. Critics of globalization tuned in announcing deviant social patterns and projecting fears of social cohesion dissipation into extremism, terrorism and dystopian versions of the future. Such fears rely indeed on facts, have been extensively argumented and are still present[4]. Robert Grovers and Frank Go, for example, stated as recently as 2009, that "*the emerging network society raises questions about the expanding digital divide and increasing social exclusion*"[5]. Grovers and Go also cite Hallowel who, a couple years earlier, in 1999, declared in more plastic terms that "*society should safegurard the "human moment", the "high touch", face to face contact between people*" *as they (people) "enjoy and need social and sensual contact; they do not want to be disembodied*"[6].

Some fourteen years later, though, **we can better see the complexities of the virtual online highly technologized environment overlapping "reality as we know it"** and may come to different conclusions. Hyper-reality remains one of the major catalysts and effects of globalization, therefore recent critics of hyper-reality have focused more extensively on its relation to the larger paradigm of globalization, nuancing their approach and understanding of effects worldwide. Same Peter Childs notes, for instance, that "*globalization operates at local and international levels, producing both cultural fragmentation and homogenization, connection and interaction, dispersal and dislocation in one connective and unifying but highly differentiated system*".[7] This ambivalent nature of globalization has also been very well expressed by Robert Rolandson, who noted that "*globalization as a concept refers both to the compression of the world and the intensification of consciousness of the world as a whole*".[8] Following Robertson we can argue that the compression of the world was the specific feature that made critics react with anxiety towards its development.

Compression brings forth an annulment of natural and agreed rhythms of change, flows of information, territorial boundaries, with huge effects on the way simulacra imprints perceptions etc. The uneasiness is felt particularly at the level of mind, as cognitive processes get altered in the process by their exposure to new frames and artificially constructed boundaries. From here, we infer, comes the negative reaction to hyper-reality and its practices, be they social, cultural, televisual or digital etc.

The second element in Robertson's depiction of globalization however has been quite celebrated by, this time, promoters of globalization. What he called ***the intensification of consciousness of the world as a whole*** has been used to announce a celebration of global participatory democracy, and a new strand of humanism in the form of active citizenship. An active citizenship that would not be possible, as we shall see, in the absence of high technology and hyper-reality. But first, let us look into what *intensification of consciousness of the world as a whole might mean...*

First, an entire array of new collective individualities loosely linked, flexible and changing. Ideologists and philosophers at the turn of the 21st century have drawn attention to the challenge represented by the many identities citizens of a global world must constantly embrace, negotiate or annul, if they are to survive. French philosopher Jacques Derrida has claimed, in the aftermath of the 9/11 terrorist attack, that global terrorism represents nothing less than the symptom of an autoimmune disease affecting Western civilization whose very existence is threatened by an increasingly inefficient mode of governance.[9]

Other writers and philosophers, perhaps not accidentally simultaneously belonging to multiple ethnic and cultural backgrounds, have attempted to see beyond the disease into a conceptual cure. The Bangladeshi British, Harvard professor of philosophy, **Amartya Sen**[10], for instance, in the widely celebrated book *Identity and Violence,* first published in 2006, **speaks of the need to permanently negotiate between our multiple identities as citizens, ethnics, culture producers, gendered individuals etc., refusing to give predominance to a unilateral strand of our enlarged personality in a global context. Amin Malouf**, French journalist and writer of Lebanese origin, speaks in fairly similar terms when deconstructing identity and its path to extremist violence in his book **On identity** (2000)[11]. **The common rhetoric is that of embracing diversity within and around us, an echo of the now declining ideology of multiculturalism that animated thinkers at the end of the 20th century.** Beyond it, remains a hope advocated by those who see in multiculturalism more than the much discussed "federation of communities" once hailed by Biku Parekh[12], with its already proven inability to promote interaction outside insulated ethnic singularities, or the now equally outdating logic of sovereign nations inherited from the Enlightenment.

An alternative, interesting, and we believe valid, answer comes from Michael Hardt and Antonio Negri, authors of “The Empire” (1999) and “Multitude. War and Democracy in the age of the Empire” (2004), **who articulate a new vision of future democracy based on the concept of multitudes.** Hardt and Negri oppose the idea of ***multitudes*** to the existing and experienced realities of ***crowd, masses or mob*** whose “*collection of differences remains inert and can easily appear as an indifferent aggregate*” and “*who cannot act by themselves but must be lead*” and are therefore” *susceptible to external manipulation*”[13]. By contrast, ***the multitude*** “*designates an active social subject, which acts on the basis of what the singularities have in common.* (It) *is an internally different, multiple social subject whose constitution and action is based not on identity or unity or, much less, indifference, but on what it has in common*”[14]. **The implications are far reaching as the multitudes challenge the entire system of sovereignty and democracy by proxy, in which leaders rule and citizens perform tasks in the hierarchical organization of society**. If viable, the model introduced by Hardt and Negri is set to produce **new forms of active citizenship**: “*The challenge of the multitude is the challenge of democracy. The multitude is the only social subject capable of realizing democracy, that is the rule of everyone by everyone*”. [15]

Such a theory is likely to attract in the coming decade strong supporters and equally strong opponents. And since it predicts a major shift in the current Western centric conceptual paradigm and an ambitious new world order, its fate can be either that of a much-applauded prophecy or an extravagant failed utopia. The dice are only starting to roll so the outcome is not to be expected soon.

From ideological diseases to conceptual cures

Given the major issues and implications at stake, it is not the aim of the current paper to assist in the philosophical conceptualization of *multitudes* or the shaping of the - we believe - emerging paradigm. My rather minor contribution would be that of **performing an exercise, finding possible instantiations of the concept. Main motivation comes from a personal observation that the concept of multitudes seems to be at**

the moment over-theorised but, unfortunately, yet underspecified. Therefore, my intention will be that of articulating it into a specific context and test its construction to see whether it can hold sense and coherence into the future. The ultimate goal – to help in the producing of a more realistic and nuanced approach to the new paradigm of thought, based on actual rather than idealized or ideologized practices and behaviours. As terrorism has been claimed by Jacques Derrida to represent *"a symptom of the autoimmune disease our society suffers from"*[16], **my intention is also to demonstrate that other types of socially aggregated movements can represent signs of cure in the new logic of multitudes**. It must be added also that this analysis is part of a larger project aimed at providing an analysis of a more comprehensive series of cultural productions and social movements that have come to transgress previous forms of thinking, putting forward what seems to be now the seeds of an emerging cultural and political paradigm, beyond postmodernity and multiculturalism.

Civic movements and social networks

Looking close at various possible manifestations of *multitudes* at the turn of the millennium I have come to the conclusion that one of the most coherent and impacting instantiations of the concept, therefore adequate to subject to a close scrutiny, is that of ***extended civic movements taking birth and shape in the virtual environment***. From the much debated Arab Spring, which wiped the Middle East throughout 2011, leaving behind a turmoiled and unstable geo-political configuration, to the very recent Turkish summer (2013) that ignited public protest against government intended destruction of a cultural symbol of lay democracy, the Taksim square in Istanbul, we have witnessed in the past two years major active citizenship and protest movements spontaneously and simultaneously sparked in the social media across the world. And with this we return to hyper-reality and its effects on our social practices and cultural productions.

No longer than ten years ago, we lived in a time of mass communication in which mainstream channels and rather fixed authorities were still guiding mappings of public choice and attitudes. In marketing studies, for example, this process was referred to as *"the one way push process of mass* *communication*"[17] in which opinions circulated towards public audience in a rather unilateral direction. What we witness today is a push and pull process in which opinions circulate freely to and fro, with citizens taking action, making their own alternative media ad hoc channels and sharing information, opinions, facts, reflecting, selecting and debating experiences via social networks sites which create an info-sphere with porous and lax boundaries. Passing form the traditional push model to the push and pull alternative media model of today presupposes a significant shift. According to Molenaar, "*a new lifestyle is emerging, characterised by mobility, fast pacedness, polyscriptedness and parallelization of experiences*".[18] This shift, implicit to globalization, has been catalysed by the **emergence of social networking services** which, as Peter Mika notes, broke forever the passive usage patterns of the "*web of the 1990's , which was a combination of a phonebook and the yellow pages*".[19] Same author records results in polls dated around 2007, which proved social networking sites to have increased dramatically the user's capacity to maintain social contacts and networks, despite recent fears of isolation and alienation. **The effect of social network sites came mostly from their facilitating active engagement and turning ratings into a form of social capital.** In addition, sites like Facebook and Twitter have offered easy solutions to create groups and share interests and a sense of simultaneous social presence and cohesiveness that today proves to have glued into active partnerships.

In addition, a sense of multitudes united by interest, able and ready to take action not only in the virtual but also in the real world seems to be the newest most relevant turnover of social networking online as the massive street protests of 2011-2012 in the Middle East and 2013 in Turkey tend to demonstrate it. **We seem to have come to a point in which citizens quickly put together and dissolve parallel experiences and communities of practice according to interest and social context.** And what's most important, they/we seem to be able to shift with increasing ease from the virtual to the real and vice-versa. The polarity announced by Baudrillard in the 90's between the real and the virtual is no longer there. In 2008, Larry Johnson predicted that over the next 15 years, we will experience the virtual world as an extension of the real one.

According to Johnson, virtual worlds were five years ago "*already bridging borders across the globe to bring people of many cultures and languages together in ways very nearly as rich as face to face interaction. They (were) already allowing the visualisation of ideas and concepts in three dimensions that is leading to new insights and deeper learning*".[20] This similar to reality quality of online interaction has turned simulacra into a real experience, in a textual grill in which real and virtual no longer oppose and compete but rather concur to the realization of a "fifth element" or dimension of our lived experience. As Pinocchio turns into a "real human" fiction body, so are we, as individuals and communities of practice, growing new flesh in an already difficult to distinguish reflection of man-robot. **And again we need to consider if what no more than five years ago seemed prophecy, namely the turning of the virtual reality into an *extension* of the real has not in the meantime been successfully accomplished only to now be turning into something else.**

But before we can answer that, and in order to better understand the paradigmatic change, let's take a look at another powerful prophecy made as early as 1967 by Michel Foucault who noted: *The present epoch will perhaps be above all the epoch of space. We are in the epoch of simultaneity: we are in the epoch of juxtaposition, the epoch of the near and far, of the side-by-side, of the dispersed. We are at a moment. I believe, when our experience of the world is less that of a long life developing through time than that of a network that connects points and intersects with its own skein.* [21] Foucault's early definition of space as the central element mapping individual and collective identities out of time and into spatial simultaneities and juxtapositions accounts in a striking way for the way contemporary experiences of identity are structured in the virtual environment, where presence is articulated into the now of the "post" and "share", regardless of geographical or temporal distances between subjects.

Another striking similarity is that between Foucault's invented term of *heterotopia* and hyperspace. In short, the French philosopher identified heterotopia[22], the other space or ultimate alterity, as being any "*real places - places that do exist and that are formed in the very founding of society - which are something like counter-sites, a kind of effectively enacted utopia in which the real sites, all the other* *real sites that can be found within the culture, are simultaneously represented, contested, and inverted. Places of this kind are outside of all places, even though it may be possible to indicate their location in reality. Because these places are absolutely different from all the sites that they reflect and speak about, I shall call them, by way of contrast to utopias, heterotopias.*" [23] So heterotopias are at the same time real and imagined places, governed by principles that contradict, contest and invert reality in all the other real sites. A close look at the way Foucault describes these places and their function across different epochs gives us a telling illustration into how space itself evolved and changed its functions in hyper-reality. According to the French philosopher, heterotopias evolved from locations at the margin of society, where crisis could be consumed outside its borders, as locations of e.g. places designated for lepers, dying people, menstruating women, into *extensions* of social space, enclosing this time deviations from the rule of the reason (from brothels to the asylum, and from the cemetery to the penitentiary).

In a similar way, hyper-reality evolved from a location of deviation at the margin of social space, isolating (and alienating) individuals that spent time entertaining themselves in a parallel universe with suspended laws, to an extension of the social space, an emplacement of inverted rigors, where the rule of law could be abolished for the creation of parallel productions. Here we have fan fiction, in which readers become authors and manipulate classical texts on their own will, as well as computer games in which wars are fought by average individuals, in much the same way in which they are televised for their entertainment.

More recent theoreticians of human geography have attracted attention to the fact that at the turn of the millennium, heterotopia has also been changing its configuration. No longer part of a grid or network in which it functions as extension containing deviation, emerging heterotopias have been acknowledged to function as places in which, this time, normality can be reclaimed out of the abnormal continuum of post (post)modernist communities. Following human geographers like Dehaene and De Cauter, we can state that in today's post civil world, heterotopias engulf, emplace and give rise to the experience of place in the non-place continuum that megacities create. "*Rather than interrupting normality, heterotopias now realize or simulate a common experience of a place*".[24] In other words, heterotopia, the simultaneously real and imagined place, living at the junction of non-space continuums, simulating places where there is only fluid space, creating and dissolving boundaries that function on imaginary maps, is now illustrated by emplacements like the mall, the cinema or the virtual world, simulating spaces of home, privacy, freedom, community etc. and thus influencing the individual and the multitudes' experience of the world. It is my belief that the concept of heterotopia will therefore prove crucial in understanding present instances of *multitudes*, their place and space in the geographies of sameness and difference, as well as the way contemporaneity can shape a new paradigm of thought.

Emerging multitude – The case of Rosia Montana or the "Romanian Autumn"

To be able to test the validity of the concept of *multitude*, its production of a heterotopic hyper-space and its impact on the social fabric, let us follow a relevant instance, less known than that of the Arab Spring or Turkish summer, but one that seems to represent a significant move forward in the new paradigm. The case under discussion is that of the Romanian born Rosia Montana protest movement (RM) started in September 2013. In the background, there is the interest in the 90's of a limited number of NGO's and civil society representatives concerned with the ecological effects of a surface mining gold exploitation project advanced by the Canadian Company Gabriel Resources at Rosia Montana in Transylvania, a region with a gold mining tradition dated since the Roman Empire. The movement has got a completely new dimension at the beginning of September 2013, when the Romanian Government introduced for approval in the Parliament a bill giving green light to the Canadian company, granting it expropriation rights on local villages, as well as the right to use massive cyanide exploitation. The bill sparked instantaneous street protests across the country, which have been lasting for the last month and a half. This was all the more surprising as Romania has not been confronted with protests of such magnitude, endurance and spreading across the country and beyond, uniting diaspora on four continents, since the mid 90's. Another significant element in our choice of RM for analysis is the fact that, unlike the Arab or Turkish protest movements, which were also spontaneously and simultaneously sparked and glued on social networking sites, this one did not happen as a result of suppression and has not followed so far a violent pattern. By contrast, the RM civic activism has been expressed in entirely peaceful ways, via weekend street marches attended by thousands of people, labeled as "Sunday in the Family", cultural manifestations as tango flash-mobs, music concerts, ad-hoc theatre plays, marathons, subway artistic sit-ins or street plaza reading sessions etc. The phenomenon is entirely unique in character and unprecedented in the Romanian society both as magnitude and ways of expression. It has been sparked and glued on the social networking site Facebook, which offered the right tool for the creation of a new type of agency, the *multitude* (in the sense granted to the term by Hardt and Negri discussed above). My intention is to show how the creation of the multitude is inextricably linked with the successful creation on Facebook of a set of narratives collectively authored and aspiring to develop into a masternarrative of the present. The narratives that sparked protest and glued active citizenship were circulated almost exclusively online, on the social network site Facebook. Mainstream media, completely taken by surprise by what was labeled as "extreme ecological movements", reacted slowly and undersized the issue for weeks. In this context, public debates, documents, scientific reports, legal arguments, ecological facts and data were mainly circulated online where they were read and debated by an increasing number of citizens. The movement grew exponentially and diversified accordingly.

In one weekend only, in early October, street protests and alternative events were organized in almost a 100 cities across the world, on four continents, being attended mostly, but not only, by Romanian diaspora representatives. For the first time since the revolution in 1989, Romanian citizens acted together and contributed to the creation of a national narrative, which invoked the right to constitutional freedom, dignity and power to choose. As we shall see, the pattern instantiated with this national event expressed globally proves that there is an urgent need to rethink traditional assumptions on the capital of power and its habitus advanced by Bourdieu[25] and his followers. **What we are witnessing, I believe, is the emergence of new forms of power making, imagining and experiencing and an increasing agency taken over by networks of citizens, or, in other words, multitudes.** It is interesting to note that the movement has had so far no political affiliation, attempts by various parties and politicians to tune in and moderate events being one by one rejected by the protesters. Other attempts on behalf of the Government, to identify leaders of the movement and start negotiations have also failed, as protesters claimed to have no leaders and not be ready for negotiations, as long as what they called “the unconstitutional bill” was not rejected by the Parliament. Critical slogans were also circulated against the entire political class.

In order to understand the mechanisms legitimating an unprecedented leaderless and large movement on the Romanian civic landscape, I will resort to an analysis of narrative productions starting from the social science view on narratology. As translations expert Mona Baker, following two reputed narratologists like Somers and Gibson notes, in social theory “*narrative is not conceived as an optional mode of communication but as the principle and inescapable mode by which we experience the world. Thus, everything we know is the result of numerous crosscutting storylines, in which social actions locate themselves*”.[26] It is the emergence and creation of these various cross-cuttings that I shall focus on in the given case of the Rosia Montana.

The Facebook narrative of the RM protests started form individual posts reflecting personal testimonials, the “I’ve been there and seen that” mode of communication. Such narratives spoke about the beauty of the place, the amount of planned destruction and the irrecoverable damage to a community and the environment. Testimonials were full of emotion and sparked interest. One of the most circulated and therefore impacting was a short movie realized by a group of passionate amateur film-makers, born and raised in the close proximity of the affected community. The film wanted to be a statement of belief about ecological damage and the need to learn from our mistakes. It was circulated extensively on Facebook as a form of warning, reminder of the cause and motivational boost and it was viewed in two weeks after its posting on You Tube by 119.786 users. It even got on National Television Channel 1 (TVR 1), where one of its producers commented it alive in debate with the owner of the advertising company responsible with the RMGC own advertising campaign. We therefore see how virtual space has facilitated and catalysed in an unprecedented way both active citizenship and individual agency which have come to compete on equal stand, in the mainstream media, for power capital with a powerful corporation and its advertising apparatus.

Such texts or storylines (be they Wordformat, visual representations, movies, art or verbal performances) are labelled in social science as ontological narratives, stories about ourselves, stories that we tell us and each other about our place in the world. They create a horizon of expectation and, when linked, as is now happening by shared interest via social networking sites, they are prone to create a collective narrative conveying a sense of closeness, community, sharing values, interests and a cause. They give a larger meaning to personal feelings and contribute to the validation of one's value and social capital via the *Like* and *Share* functions.

Once the sense of interest was sparked and the network expanded the number of online Friends across the country and the world, people who have had no physical encounter, related and empowered each other's stories. In a matter of days, via Likes and Share, individual people became brands, followed, appreciated and therefore encouraged and legitimated to post on behalf of a growing hyper-textualised community.

Once the community enlarged, experts began to contribute to the narrative, feeding legal, economic, historical, cultural cross-cutting storylines in the making of the shared narrative, which slowly turned into a collective ontological narrative adhered to by people in search of a national identity model. Reasons explained, circulated and debated on the social platform added up to each other, as history lovers, artists, ecologists, people preoccupied by the cultural heritage tuned in. Motivations were expressed in terms of dignity, solidarity, shared interest to preserve a common cultural heritage dating from 2000 years ago, need to prevent an ecological disaster potentially affecting half of the country etc. Once subscribed to, these stories created what I would call a growing national narrative, which has been guiding the behaviour of thousands of people that took to the streets with unexpected resilience. Its impact and power comes from the fact that in a highly technologized world, in which people expect events and public positions to be at least partially, if not completely shaped by advertising and PR specialists, political positions to be mediated and forged by multiple interests, including electoral ones, **social media is still perceived as unmediated, spontaneous, impossible to forge.** It is worthwhile remembering that two decades ago, in the age of television dominance, the TV "No Comment" news collection or the "World in Pictures", as a famous photo reportage on CNN on line was called, were successful for precisely the same reason. They conveyed the impression of real life, unmediated reality, objective transfer of events right from the heated heart of the "happening" into the comfortable sitting room of the average citizen. The emergence of digital photography ended its instrumentalisation as powerful and neutral mirror of reality and made perceptions of televisual choreography even more acute. In this context, social media with its new tools that allow the average individual tune in and bring his/her own contribution to a the shared orchestration, have produced, and I suspect will increasingly produce, instances of citizen agency and empowerment in unprecedented forms and intensity.

In the particular case of the given protest, the collective ontological narrative created the premises for the emergence of the first major national public narrative elaborated by and circulated among non-state formations and even despite the state. This is all the more significant as narratologists advocate "*social organization, social action and social identities*" to be constructed "*through both ontological and public narratives*".[27] Implications are all the more significant as once coherence reached, such narratives help in embedding meanings of future events in a shared framework of perception in which previous models can be delegitimized at great speed and with significant consequences to social formations.

The narrative of RM crossed national boundaries in less than two weeks and was reclaimed in equal sense by representatives of the diaspora that organised ad hoc events of solidarity in Europe, Canada, the US, Australia and Hong Kong. This, again, was an unprecedented reaction, no other event, call for action or cause having attracted such coherent participation from the diaspora in the last 20 years.

Their photographic, filmed testimonies and motivational postings were subsequently shared with increased speed among FB users, therefore contributing to the enlargement of the target audience. Object-specific slogans such as "*United we save Rosia Montana*", "*We want culture, not cyanide*" and "*We want clean waters, not cyanide pollution*" turned increasingly to emotional identification of the RM cause with the country and the world. From week 3, when the diaspora increased in visibility, slogans included "*Rosia Montana is Romania*", "*Hands of our future*" , "*Rosia Montana is the World*", and "*The Future has a collective author*", making from a local cause and a remote location on the borders of Europe the centre of an aspiringly global stand against pollution, economic suppression of ecology and corporate intervention in law making.

We can therefore see how in less than a month, the individual ontological narrative of a small number of people can turn into a glocal theme promoted and embedded at the interstice of a very varied number of social contacts and networks. Subsequently, the RM cause was shared by individuals affected by similar exploitations as well as those fighting similarly perceived dangers (e.g the Slovac movement "Kremnica nad zlato - Kremnica beyond gold")[28].

Its force can be traced in the successful embedding of a number of different strands of discourse, from the ecological, to the legal, from the historical to the cultural and from the defence of constitutional rights to expression of national identity across borders. An analysis of individual postings before and after joining the RM protests shows that those attending it are obviously motivated in different ways and have different views on life. Some are strong nationalists, some advocate for an eco-friendly future, some are historians and some fight for the preservation of the cultural heritage. And most seem to be average citizens caught in by a sense of urgency and immediacy, of irreparable damage affecting important strands of individual and collective identity.

The Save Rosia Montana movement is thus a clear example in which one story has come to engulf multiple significances beyond its initial configuration. Stating with David Herman that "*storyworlds are global mental representations enabling interpreters to frame inferences about the situations, characters, and occurences, either explicitly mentioned or implied by a narrative text or discourse*"[29], we can move forward in our analysis and prove the world creating potential of the narrative in general, and this narrative in particular. It seems to convey a significant capacity to weave complex reading grids and therefore offer a model of thinking that will undeniably guide interpretation of future events.

A model is emerging with increased clarity. Social networking sites create the environment, the illusion of space in the non-place continuum, allowing individual and collective agency express desires and ideals of home, patriotism, freedom, purity etc. Once emplaced, these features of a once hyper-real architecture begin to grow a body of their own, moving at the will of everyone and the multitude at the same time. This power to evolve rather unpredictably is the one that opens up space, blurring contours between what's simulated and what's real, allowing hybridizations and cross-fertilizations as in the case of the Rosia Montana movement. Real and simulated interactions between individuals, real world activism and virtual statements blend in a continuum and give us a taste of future social patterns and behaviours. What we will witness in the coming period will most likely be the emergence of a new masternarrative of active citizenship in search of meaningful causes. Ecology seems to be one of the most promising, as is the new democracy of the multitudes. Nevertheless, as mentioned, the dice are only starting to roll, the outcome being yet undetermined...

How will intelligence agencies be affected remains to be seen. For now, we can note an urgent need to rethink patterns of risk, understand factors of change in the emerging conceptual paradigm and learn to train our ability to detect storylines' potential of creating master-narratives of change, those likely to cross geographical boundaries with great speed and affect the lives of everyone.

References

[1] Jean, Baudrillard, 'The Gulf War Will Not Take Place' (first publ. in *Libération*, 4 Jan. 1991), "The Gulf War: Is It Really Taking Place", (first publ. in *Libération*, 6 Feb. 1991) and "The GulfWar Did Not Take Place" (first publ. in *Libération*, 29 Mar. 1991) in Baudrillard, Jean, The Gulf War Did Not Take Place, (Bloomington: Indiana University Press, 1995), pp. 23-87.

[2] Peter Childs, *Texts. Contemporary Cultural Texts and Critical Apro*aches, (Edinburgh University Press, 2006), p. 76.

[3] see for instance Douglas Kelner, *The Persian Gulf TV War*, (Bolder Westview Press, 1992); Paul Virilio, *Desert Screen, War at the Speed of Light*, (London, Continuum, 2002), and Slavoj Zizek, *Welcome to the Desert of the Real!, Five Essays on September 11 and Related Dates,* (Verso: UK, 2002).

[4] Jurgen Habermas and Jaques Derrida, provided an acute analysis of the Enlightenment heritage and the construction of modernism into the present day in Giovana Borradori (ed), Philosophy in a Time of Terror, Dialogues with Jürgen Habermas and Jacques Derrida, (Chicago and London: University of Chicago Press, 2003).

[5] Robert Graves and Frank Go, *Place Branding, Glocal, Virtual and Physiscal Identities, Constructed, Imagined and Experienced*, (Palgrave Macmillan, UK, 2009), p. 3.

[6] Hallowel E. M., *The Human Moment at Work, apud* Robert Grabes and Frank Go, *op. cit.*

[7] Peter Childs, *op. cit.*, p. 156.

[8] Robertson Roland, *Globalization: Social Theory and Global Culture,* (London, Sage Publications, 1992), p. 8.

[9] "Autoimmunity: Real and symbolic suicides – a dialogue with Jacques Derrida" in G. Borradori (ed.), *Philosophy in a Time of Terror – Dialogues with Jurgen Habermas and Jacques Derrida*, (Chicago and London: University of Chicago Press, 2003), pp. 134-135.

[10] Amartya Sen, *Identity and Violence, The Illusion of Destiny*, (Penguin Books, UK, 2007).

[11] Amin Malouf, *On identity*, (Haberville, Panther, 2000).

[12] Biku Parekh, „Defining British National Identity", *The Political Quarterly*, Volume 71, Issue 1, pages 4-14, January 2000.

[13] Michael Hardt and Antonio Negri, *Multitude. War and Democracy in the age of the Empire*, (New York, Penguin Press, 2004), p. 101.

[14] *Ibidem*.

[15] *Ibidem*.

[16] "Autoimmunity: Real and symbolic suicides – a dialogue with Jacques Derrida" in G. Borradori (ed.), *Philosophy in a Time of Terror – Dialogues with Jurgen* Habermas and Jacques Derrida, (Chicago and London: University of Chicago Press, 2003), pp. 134-135.

[17] C. Molenaar *apud* Robert Graves and Frank Go, *Place Branding, Glocal, Virtual and Physiscal Identities, Constructed, Imagined and Experienced*, (Palgrave Macmillan, UK, 2009), p. 49.

[18] *Ibidem*.

[19] Mika Peter, *Social Networks and the Semantic Web*, (Springer, 2007, USA), p. 21.

[20] Johnson Larry *apud* Derek S. Reveron, ed., *Cyberspace and National Security, Threats, Opprtunities and Power in a virtual World*, (Georgetown University Press, Washinton, US, 2012), p. 5.

[21] Foucault Michel, *Of Other Spaces, from "What is an Author?*, in *Language, Counter-Memory, Practice*, (Cornell University Press, Ithaca, New York 1977), pp. 124-127, p. 124.

[22] from gr. *heteros*=other and gr. *topos* = place

[23] Michel Foucault, "Of Other Spaces, from "What is an Author?", in *Language, Counter-Memory, Practice*, Cornell University Press, Ithaca, New York 1977, pp. 124-127, p. 126.

[24] Michiel Dehaene, *Lieven De Cauter - Heterotopia and the City Public Space in a Postcivil Society*, (Routledge, London, UK, 2008), p. 5.

[25] Pierre Bourdieu , *The forms of capital* in J. Richardson (Ed.), *Handbook of Theory and Research for the Sociology of Education*, (New York, Greenwood), pp. 241-258.

[26] Mona Baker, „Narratives in and of translation", 2005, *Skase Journal of Translation and Interpretation*, vol. 1, no. 1, 2005, pp. 4-13, retrieved from www.skase.sk, p. 5.

[27] *Ibidem*, p. 6.

[28] Information available at https://www.facebook.com/events/199558763549124.

[29] David Herman, "Narrative Ways of Worldmaking", in Sandra Heynen and Roy Sommer (ed.), *Narratology in the Age of Cross-Disciplinary Research*, (Walter de Gryuter, Berlin, 2009), pp. 71-87.

Bayesian Intelligence Analysis

Davide BARBIERI[*]

Abstract

Statistics and probability are basic tools of data analysis and are often used in government and business intelligence to synthetically describe the domain of interest and to make inferences and predictions. Still, even the basic theory of probability, in its classic form, is not necessarily intuitive or bias-free, especially when it comes to conditional probability. Bayesian inference is a subjective and alternative way of looking at it, which may be taken into consideration when added information is available, in order to mathematically quantify the analyst's perceived risk. This paper reviews its possible applications to intelligence analysis, especially for strategic warning tasks.

Keywords: Inferential statistics, conditional probability, Bayesian inference, data analysis.

Introduction

Descriptive statistics is a set of mathematical tools for analyzing data. It is usually adopted in order to outline synthetically a domain or problem of interest. In case analysts have to analyze large amount of data, they can use some indexes of central tendency, like the mean or the median, and of dispersion, like the standard deviation or the range, to summarize a situation. Analysts in fact produce syntheses and reports, which can be forwarded to decision makers and stakeholders.

Inferential statistics instead can be used to make predictions, that is to draw conclusions (inferences) from a given set of data, that analysts hope to be as large as possible. In fact, the accuracy of a prediction largely depends on the amount of available data, since an inference is drawn in an inductive way, from (possibly many) details to a general conclusion. While in pure mathematics we learn by means of deductive reasoning from a set of general axioms and rules, in inferential statistics we learn from experience (historical data) and by means of inductive reasoning.

Predictions are based on probability, the estimate of the chances that something will happen. In intelligence analysis, probability can be used to predict wars, military coups or terrorist

[*] Dr., University of Ferrara, Italy

attacks. In business intelligence, it is used to predict bankruptcy, new trends, customer behavior and sales. While in case of large data sets we can apply data mining methods and technologies, very often in intelligence analysis analysts cannot rely on large amount – in statistical terms - of historical data. Therefore, classic statistical inference may have a limited application, especially in strategic warning, where a single item of intelligence could modify the perceived risk of an event.

Also, probability can be very counterintuitive - regardless of what people untrained in statistics may think - and it is often prone to some biases, especially when it comes to conditional probability. The topic of this paper is a peculiar way of conceiving conditional probability - and therefore inferential statistics -which does not necessarily rely on large amount of data. The main objective is to understand whether the proposed approach can be satisfactorily applied to intelligence analysis.

Different ways of looking at probability

There are three basic ways of defining probability. The first one, in historical terms, was made famous by French mathematician Laplace: it says that the probability *P* of an event *E* is the number of favored cases *m* divided by the total number of possible cases *n*:

$$P(E)=m/n$$

This classic definition can be applied when all the possible elementary outcomes of a random trial (or experiment) are known and each of them has the same chances of happening (which causes the definition to be a bit elliptical, since probability and chance are synonyms). For example, the probability that the roll of a die will give an even number is *3/6=1/2*. There are in fact 6 numbers in a die, 3 of which are even. The 6 numbers taken together constitute the set Ω of all the possible outcomes, that is the *sample space*.

An important property to remember is that the probability of an event is always between 0 and 1:

$$0 \leq P(E) \leq 1$$

If *P(E)=0* then the event is impossible (for example, the event that a die roll will give 7). If *P(E)=1* instead, the event is certain (for example, the probability that a die roll will give an even or an odd number, or the outcome will be between 1 and 6).

This first approach has evident limits. In fact, outside gambling, there are many cases in which not all the possible outcomes are known, or it is not known whether they all have the same chances. In such cases, a second way of thinking about probability can be adopted: the *frequentist* approach. The frequency *f(E)* of an event is the number of times it occurs. Its relative frequency is the number of times it occurs out of *n* trials: *f(E)/n*. For example, an airplane crash has a very low relative frequency, given the large amounts of flights occurring, which means it has a very low probability (compared to the opposite event, that the airplane lands safely). In fact, if *n* becomes very large, then the relative frequency approaches theoretical probability:

$$\lim_{n\to\infty} f(E)/n = P(E)$$

This is the famous “law of large numbers”. This definition has been consistently adopted by Austrian engineer Von Mises and epistemologist Popper. According to Von Mises, the frequentist approach is suitable if there are sufficient reasons to believe in future stability, that the relative frequency of the observed events will lead to a fixed limit if the observations were continued indefinitely (Schield and Burnham 2008). Von Mises though seemed to overlook the fact that indefinite may be very short from infinite.

If we have a large collection of data (as in the case of the so called *big data*), stored in a database or a data warehouse, the frequentist approach can be useful in order to make predictions, as it is currently being done in data mining, e.g. with classification algorithms. Unfortunately though, especially in intelligence analysis, the number of cases at hand can be very low. Definitely, it will never be infinite, therefore this second definition cannot apply, strictly speaking: the frequency that analysts observe will never coincide with probability.

There is a third, subjective way, of defining probability: the degree of confidence that a subject will assign to an event based on available information, previous experience or personal evaluation. But how can we quantify the probability according to this non-mathematical definition? A possible solution could be the gambling method: How much would you bet on an event, relying on your information? This approach to probability and predictive inference has been proposed, among the others, by Italian mathematician De Finetti (1972, 1974).

In real life situations, people tend to adopt this approach very often (Tverskyand Kahneman1971, Kahneman and Tversky1972). If an insurance agent knew that an airline company has obsolete airplanes and poor maintenance, would he still consider probability in purely frequentist terms? Or would he subjectively lower his degree of confidence, revising the probability of a crash according to the perceived risk, thus increasing the insurance premium?

Conditional probability

Things may become even less obvious when we move from simple probability to conditional probability, which is defined as the chances that an event will occur *given another event* which has already occurred: $P(A|B)$, which can be read as the probability of *A given B*. The following is the classic definition:

$$P(A|B) = P(A\ and\ B)/P(B)$$

Where $P(A\ and\ B)$ represents the *joint probability of* $A \cap B$, the intersection of the outcomes of A and B.

The definition of conditional probability is still a probability according to Laplace. In fact, $A \cap B$ are the favored cases, while $B$are the possible cases, according to the imposed condition: in case B is true, it represents the new possible cases (Ω).

The probability of any given number in a fair die is 1/6. The joint probability that the roll of a die will give an even number n greater than 3 is $P(A \cap B)$, where A is the event "*n is even*" corresponding to the following outcomes: {2, 4, 6}, and B is the event "*n>3*" corresponding to {4, 5, 6}. Therefore, their intersection is$(A \cap B)=\{4, 6\}$, and the corresponding joint probability is calculated as 2 favored cases out of 6 possible: $P(A \cap B)=2/6=1/3$(see Figure 1).

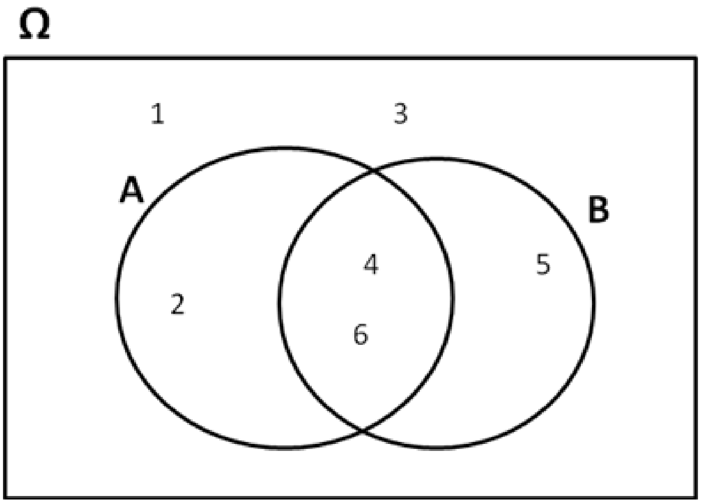


Figure 1 – Joint probability

Since the probability of *B* is *P(B)=3/6=1/2*, then, applying the definition, the conditional probability that *n* is even given *B* is *P(A|B)=P(A∩B)/P(B)=(2/6)/(1/2)=2/3*. In fact there are 3 numbers which are greater than 3 in a die: {4, 5, 6}, 2 of which are even: {4, 6}.

If the two events are independent, i.e. the probability of one does not affect the probability of the other to happen, then their conditional probability is *P(A|B)=P(A)* and *P(B|A)=P(B)* by definition. In this case, we can easily calculate their joint probability, that is the chances of *A* and *B* to be true at the same time, from the previous definition of conditional probability:

$$P(A \cap B) = P(A)P(B)$$

As an example of independent events, we can take two fire detectors which have been installed in the same room. The probability that detector A fails in case of fire is *P(A)=0.03*, while the probability that detector B fails is *P(B)=0.02*. What is the probability that both fail and no alarm is given? Most people may think that the risk in case of fire is still very high (Heuer 1999, p. 123), but the mathematically correct probability is just $0.03 \times 0.02 = 0.0006$ or the 0.06%, which means that the alarm will fail only 6 times out of 10000 fires, a much lower risk than in case of just one detector. Intuitively, multiplying two relatively high probabilities does not account for such a low result.

The conditional probability that the second one fails, given that the first has failed, is:

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{P(A)P(B)}{P(A)} = P(B) = 0{,}02$$

that is its simple probability, since the two events are independent.

To verify how counterintuitive conditional probability can be, try the following: toss two coins and ask what the probability is that both are head (event *A*), given that one is certainly head (condition *B*). Most people will reply 1/2 or 1/4,but neither is the correct answer. The joint probability of “having 2 heads”(A) and “at least one head” (B)is *P(A∩B)=P(A)=1/4*, since there are 4 possible outcomes, only one of which is “2 heads”. The probability of having at least one head is *P(B)=3/4*, since there are 3 favored cases out of 4 possible (see Figure 2). Therefore, the conditional probability of having 2 heads, given that at least one is head, is *P(A|B)=(1/4)/(3/4)=1/3*.

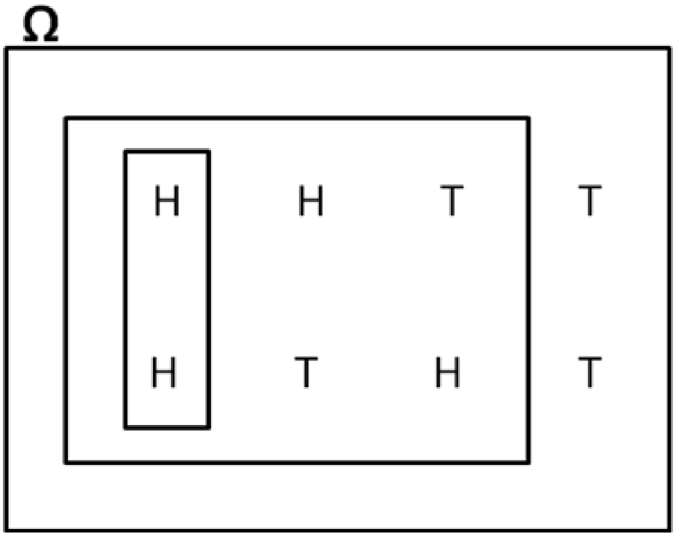


Figure 2 – Conditional probability (H: head, T: tail)

Regardless of the fact that conditional probability may be counterintuitive, we use it – or assume it – very often. For example, in the toss of a coin we say that head and tail have both the same probability, that is 1/2, *given that the coin is fair*. If we could not make this assumption, then the individual probability of head and tail should be re-evaluated. So we can reverse the problem: What would you think if, in 10 tosses of a coin, you got 8 heads? Would the assumption of fairness still be probable? Or would you revise it? Just consider that 10 is very short from being a "large number".

Bayes' rule

In science, and medicine in particular, researchers may want to know the probability of an event given some evidence. Physicians may want to calculate the probability of a disease given a symptom or the result of a clinical exam. For example, they may want to know the probability that patients have a heart attack (hypothesis H) if their blood pressure is high (event E, the evidence, the known information). Using the definition of conditional probability, they have to calculate:

$$P(H|E)=P(H\cap E)/P(E)$$

Scientists may not know the joint probability of H and E, which is needed to calculate the expression above. In fact, $P(H\cap E)$ is not so obvious, especially in case of two dependent events like disease and symptom. We have therefore to find a different way of looking at conditional probability.

Since intersection is commutative then:

$$P(H\cap E)=P(H|E)P(E)=P(E|H)P(H)$$

Therefore, the expression of the conditional probability of H given E can be written in the following way:

$$P(H|E) = P(E|H)P(H)/P(E)$$

which is the rule of Bayes, the British mathematician who stated it in the 18th century. It is not a theorem strictly speaking, since it is an identity of immediate demonstration, stemming from a property of intersection.

$P(H|E)$ is the *posterior*, or revised probability, the probability of P given (that is, after observing) evidence E. $P(E|H)$ is called the *likelihood*, the conditional probability of E in case of H (i.e. the probability of observing the symptom in case a subject is really ill), while $P(H)$ is the *prior*, the probability of *Ha priori*, without having any information on E (i.e. the probability of the disease in the general population, not only in those subjects who have symptom E). $P(E)$is the given information, the probability of observing E in the population i.e. its *marginal probability*. In case of two mutually exclusive events, like disease or not disease, it can be defined as follows:

$$P(E)=P(E\cap H)+P(E\cap \text{not } H)=P(E|H)P(H)+P(E|\text{not } H)P(\text{not } H)$$

The rule can be applied also to the previous example of two coins, one of which is certainly head. In fact, the likelihood of having one head given that both coins are head is $P(E|H)=1$ (certainty), while the prior probability of having two heads is $P(H)=1/4$, and the probability of having at least 1 head is $P(E)=3/4$. Therefore the conditional probability of having 2 heads given that one is certainly head is $P(H|E) = (1 \times (1/4))/(3/4) = 1/3$, as with the traditional approach. But this is a trivial example, in which the rule of Bayes is of no real help, since it falls within the definition of classic probability, where all possible outcomes are known and have the same chances. Unfortunately, things are not so obvious in cases where the probability of all possible outcomes are not known, as with the hypotheses of disease or not disease.

Still, likelihood is usually a simpler value to find and it is often used in diagnostics. In fact, applying Bayes' rule we are approaching the problem of estimating the probability of a disease given a symptom from the opposite point of view, that is looking at the probability of observing the symptom given the disease. Medical doctors may know $P(E|H)$, that is how many times (in frequentist terms), in case of illness H, symptom E was present. They may get it from previous experience or from a large historical data repository.

An example may help to understand the variables defined above. In a population of 100 individuals, the probability of having a certain disease is $P(H)=10/100$, which in diagnostics is called the *base rate*. As a consequence, the probability of not having the disease is *P(not H)=90/100*. Doctors also know – thanks to further investigations - that given a positive test *E*, 9 out of 15 subjects were ill (the true positives, TP), while 6 were not (the false positives, FP, that corresponds to false alarms or type I errors). Further, among the 85 people who were not positive, 84 were correctly diagnosed as not ill (the true negatives, TN), while 1 was ill (the false negative, FN, that corresponds to amiss or type II error).Unfortunately, no medical test is perfect. A contingency table can be used to sum up this situation:

Table 1 – Contingency table

	H	**Not H**	
E	9	6	15
Not E	1	84	85
	10	90	100

From Table 1 it is easy to calculate the joint probabilities, dividing the value of a cell by the total number of individuals. Therefore, the probability of being at the same time ill and positive is *P(H∩E)=9/100*, while the probability of being ill and not positive is *P(H∩not E)=1/100*. The probability of being not ill and positive is *P(not H∩E)=6/100*, while the probability of being not ill and not positive is *P(not H∩not E)=84/100*.

The marginal probability of being positive is easily calculated summing the values of row *E* and dividing by the total number of individuals: *P(E)=15/100*. The marginal probability of being negative is *P(not E)=85/100*. Similarly for the probability of being ill: *P(H)=10/100*, or not ill: *P(not H)=90/100*.

The conditional probability of being positive if ill is:

P(E|H)=P(E∩H)/P(H)=(9/100)/(10/100)=9/10

which is equivalent to the *sensitivity* of the test, the ability to correctly identify those with the disease, or *true positive rate: TPR=TP/(TP+FN)=9/(9+1)=9/10*.

The conditional probability of being positive if not ill is instead:

P(E|not H)=P(E∩not H)/P(not H)=(6/100)/(90/100)=6/90 which is equivalent to the *false positive rate:* $FPR=FP/(FP+TN)=6/(6+84)=6/90$.

The conditional probability of being not positive if not ill is:

$P(not\ E|not\ H)=P(not\ E\cap not\ H)/P(not\ H)=(84/100)/(90/100)=84/90$

which is equivalent to the *specificity* of the test, the ability to correctly identify those without the disease, or *true negative rate:* $TNR=TN/(TN+FP)=84/(84+6)=84/90$.

The conditional probability of being not positive if ill is instead

$P(not\ E|H)=P(not\ E\cap H)/P(H)=(1/100)/(10/100)=1/10$

which is equivalent to the *false negative rate:* $FNR=FN/(FN+TP)=1/(1+9)=1/10$.

The conditional probability of being ill if positive is:

$P(H|E)=P(H\cap E)/P(E)=(9/100)/(15/100)=9/15$

which is equivalent to the *positive predictive value:* $PPV=TP/(TP+FP)=9/(9+6)=9/15$.

The conditional probability of being not ill if not positive is instead:

$P(not\ H|\ not\ E)=P(not\ H\cap not\ E)/P(not\ E)=(84/100)/(85/100)=84/85$

which is equivalent to the *negative predictive value:* $NPV=TN/(TN+FN)=\ =84/(84+1)=84/85$.

Ideally, doctors would like to maximize both sensitivity, thus minimizing false negatives (type II errors), and specificity, thus minimizing false positives (type I errors). Unfortunately, they have to accept the trade off: raising sensitivity will increase false alarms and raising specificity will increase misses.

In a real situation, doctors usually do not know joint probabilities. Usually though, they know the base rate of the disease $P(H)$ and therefore $P(not\ H)$, the true positive rate of the test (the likelihood) and the false positive rate. In the previous example $P(H)=1/10$, $P(not\ H)=9/10$,$P(E|H)=9/10$ and $P(E|notH)=6/90$. Now we can calculate the conditional probability of having the disease given a positive test, i.e. its positive predictive value, by means of the rule of Bayes:

$$P(H|E)=\frac{P(E|H)P(H)}{P(E)}=\frac{P(E|H)P(H)}{P(E|H)P(H)+P(E|not\,H)P(not\,H)}=\frac{\frac{9}{10}\times\frac{1}{10}}{\left(\frac{9}{10}\times\frac{1}{10}\right)+\left(\frac{6}{90}\times\frac{9}{10}\right)}=\frac{9}{15}$$

or 60%, which corresponds to a rather low positive predictive value, given a relatively high true positive rate and low false positive rate. In fact, in case the disease is rare, i.e. it has a low *P(H)*, then the probability of the patient being ill - even if the test is positive - is low.

On a margin, if we had a test giving no false positives, i.e. *P(E|not H)=0*, then the probability of having the disease in case of a positive test would be 1, that is certainty:

P(H|E)=P(E|H)P(H)/P(E)= P(E|H)P(H)/(P(E|H)P(H)+P(E|not H)P(not H))= P(E|H)P(H)/(P(E|H)P(H)=1.

Eddy (1982) used a similar example, with a much lower base rate (*P(H)=0.01*) with a true positive rate of 0.8 and a false positive rate of 0.1. He found that 95% of the physicians estimated that the probability of having the disease, given a positive test, was between 70% and 80% while applying Bayes' rule, the correct result is only 7.5%. Possibly, they were confounding the positive predictive value (which they were asked to estimate) with the higher true positive rate.

The adoption of Bayes' rule acknowledges the fact that we are prone to change our prior estimate as more information (test results, evidence etc.) becomes available. In this sense, Bayes probability is close to the subjective definition. This situation is recurrent in intelligence analysis. In this trade, analysts may want to calculate the probability that a war or some crime, terrorist attack etc. (the equivalent of a disease in medicine) is going to happen, given an event *E* (the equivalent of a symptom in diagnostics) which has just occurred, like a political crisis, an economic collapse, a failed diplomatic negotiation etc. They may actually estimate the likelihood from historical record, that is how many times event *E* was observed in case of war.

Applying Bayes' rule, analysts can calculate the conditional probability of two competing hypotheses, H_0 (no war is going to happen) and H_1 (there is going to be war): $P(H_0|E)$ and $P(H_1|E)$, which is actually what intelligence analysts are expected to do. In this way the prior expectations of war are updated according to a new evidence, i.e. an item of intelligence.

Bayesian inference in intelligence analysis: a historical perspective

In a paper by Zlotnick (1970), Bayes' rule is simply defined in the following terms:

$R = PL$

where R is the posterior, or the estimate of the conditional probability of hypothesis Hafter revising the latest evidence E. R is equal to P, the prior estimate (which is given) times L, the likelihood ratio of event E in case hypothesis H is true:

$L=P(E|H)/P(E)$

that is the analyst's evaluation of the diagnostic importance of an item of evidence. E is diagnostic if its conditional probability is different in case different competing hypotheses are true. For example, if an observed deployment of troops (evidence E) is considered to be twice more likely in case of imminent war than in case of no war, then the likelihood ratio is 2/1.

R is the result of a mathematical processing and represents the theoretical probability according to the analyst's view of the events. It is a conclusion that follows automatically, calculated by means of a computer, and it is stored inside the memory. In case more evidence is available, it becomes the prior of the subsequent run, recursively.

The author suggests that the area of intelligence analysis where the Bayesian approach can be adopted is strategic warning, where analysts must give the probability of an imminent terrorist attack or war (Pearl Harbor in 1941 or the invasion of South Korea in 1950 could have been possible cases).

On the positive side, the author lists the following:

- The adoption of Bayesian analysis can force intelligence analysts to quantify their estimates, which they usually express in non numerical terms (Heuer 1999, pp. 152-156), thus reducing the risks of misunderstanding.
- It may reduce cognitive biases, since Bayes' rule compels to evaluate a set of alternative hypotheses, not just one, like in strategic warning, where both the probabilities of war and no war must be evaluated.

- Analysts are usually better at evaluating a single piece of evidence at a time rather than at drawing inferences from a large body of evidence (data mining was not established yet).

On the negative side, the author lists the following problems:

- The limited life span of evidence, since a piece of information collected in January does not have the same value in February. People and governments change ideas.
- The counterintuitive reversal in the relationship between cause and effect. As an example, the author cites president Kennedy warning the USSR in 1962 about the deployment of missiles to Cuba. An uncritical Bayesian may think that this is the evidence that the risk of war has increased ($L>1$), while it is obvious that the president wanted to lower it with that sort of statements.
- The risk of including false evidence in the analysis. Still, this problem affects also traditional analysis.
- Probably, a pragmatist analyst will keep thinking that an increased amount of evidence will improve the accuracy of his/her analysis more than any formal logic, like Bayes' rule. Still, gathering more information is not always possible, and intelligence must use what it has.

The author's conclusion is that Bayesian inference can significantly improve the area of strategic warning, supporting or contradicting traditional analysis.

In August 1969 the CIA had to evaluate the hypothesis that the USSR would attack China within the following month, in order to destroy its alarming nuclear capabilities. Analysts were directly asked to make an estimate, that is to evaluate the probability of a war. Their assessments were asked again every week. The perceived risk of a war slowly diminished and at the end of September it was clear that the USSR was not going to attack China (Fisk 1972).

In order to evaluate the opportunity offered by a Bayesian approach, a list of independent events (or items of intelligence)E_1, E_2… E_n was compiled. For example, event E_1meant that Soviet reservists had been called on active duty, E_2that there had been anti Chinese propaganda from the Soviet side and so on. Then the analysts evaluated from their past experience the like lihoods

$P(E_i|H)$of E_1, E_2... E_n in case of a war. Furthermore, the analysts were asked to revise their estimates, applying Bayes' rule. The added information on the event slowered quickly the perceived risk of a war, which actually did not happen. Week after week, Bayesian probabilities always fell below conventional probabilities, demonstrating a better predictive accuracy. The qualitative trends of both inference methods are shown in Figure 3.

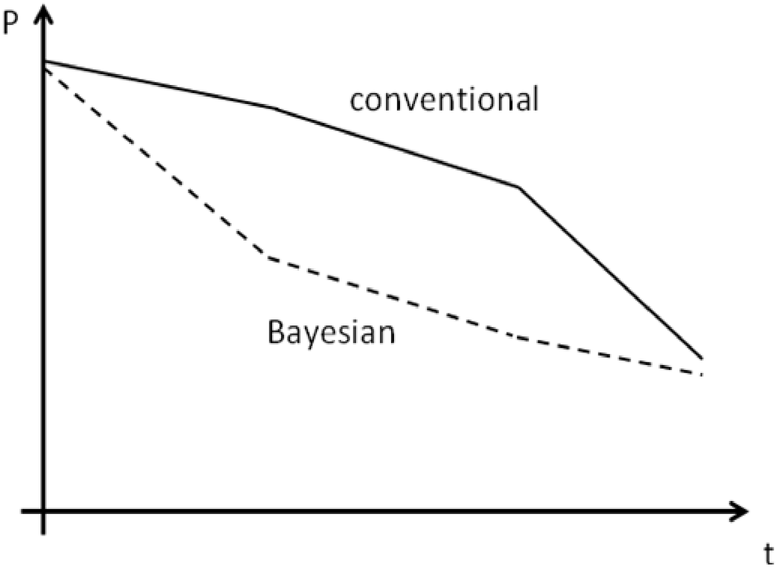


Figure 3 – Conventional and Bayesian probabilities (adapted from Fisk 1972)

In 70's of the last century, the "information explosion" problem was already perceived as a risk and an opportunity, requiring computational resources to be tackled and leveraged. In this context, a study by Schweitzer (1976) described an attempt to adopt a Bayesian approach to intelligence analysis. The author explained Bayes' rule as a way to revise the probability of a hypothesis in case of additional information. In the experiment described by the paper, the analysts had to verify the probabilities of two competing hypotheses: that Israel was not going to attack Syria

(H_0, the null hypothesis) or that Israel was actually going to attack (H_1, the alternative hypothesis). Being two complementary events, the sum of their probabilities had to be 1.

The prior probabilities of the two competing hypotheses were set to $P(H_0)=0.9$ and $P(H_1)=0.1$, with war being unlikely. An additional piece of information was then revealed: "Israeli finance minister Rabinowitz stated that the nation's economic situation is one of war and scarcity, not one of peace and prosperity". After hearing the minister's statement on the radio, the two likelihoods of such an event were estimated by the analysts as $P(E|H_0)=0.8$ (in case of no war) and as $P(E|H_1)=0.99$ in case of war. Then they had to apply Bayes' rule and revise the probability of an attack accordingly:

$$P(H_0|E) = P(E|H_0)P(H_0)/P(E) = 0.8 \times 0.9/0.819 = 0.88$$

$$P(H_1|E) = P(E|H_1)P(H_1)/P(E) = 0.99 \times 0.1/0.819 = 0.12$$

where

$$P(E) = \sum_{i=0}^{1} P(H_i) \times P(E|H_i) = (0.9 \times 0.8) + (0.1 \times 0.99) = 0.72 + 0.099 = 0.819$$

The perceived risk increased consistently according to the analysts' view.

To summarize, given the initial probabilities of two mutually exclusive events, that there is going to be no war or that there is going to be war, that is $P(H_0)$ and $P(H_1)$, and given the analysts' assessments of how likely an event E would be in case of each of the two hypotheses, $P(E|H_0)$ and $P(E|H_1)$, then the revised probability, after event E has been observed, can be easily calculated applying the rule.

In this study, analysts were particularly good at predicting non-events, proving that the evidence did not support the hypothesis of war. The Bayesian approach though showed this trend earlier than the analysts' traditional intuitive method. The author assigned great importance to the possibility of displaying graphically the results of the analyses. He affirmed that charts are much better at illustrating trends than words and supposed that much of the success of the reports could be due to this reason rather than to the technique itself.

Schweitzer's view is that the rule of Bayes is simply an "organizing device", allowing analysts to use their expert opinions on a situation to assess numerically the probability of an event. Among the main benefits he listed the following:

- Bayes' rule allows each piece of evidence to add its weight, even if limited, to the final assessment in a consistent and systematic way.
- It helps resolving disagreements, which can be seen as different points of view over the weight of an evidence, and not as non-surmountable differences on the final judgments.
- The rule helps the analysts to evaluate different competing hypotheses, not just one.
- It compels the analysts to quantify their judgments - avoiding ambiguous statements - and allows to graphically display them.
- The rule provides less ambiguous assessments, while with the traditional method analysts tended to "shoot in the middle", leaving more room for the interpretation of their opinion.
- Analysts had to periodically update the calculation considering new evidence, which assured the managers that the problem at hand was being consistently and effectively monitored.

According to the author, the limitations in the applicability of the technique were:

- The problems must be stated in terms of mutually exclusive hypotheses.
- In this process, the questions may become too simplistic, as the consequent answers.
- There must be a continuous flow of information related to the questions, in order to revise the probability *a posteriori*.

The author's conclusion is that Bayesian inference can be a valid support to the traditional methods of intelligence analysis, even if many of the problems that analysts face can fall outside the limited scope of the rule.

Conclusions

Conditional probability – and Bayes' rule in particular – can be rather counterintuitive. Nonetheless, evaluating the chances of competing hypotheses, given some evidence or collected information, is what intelligence analysts are required to do. The studies in diagnostics and intelligence analysis seem to prove the effectiveness of Bayesian inference in helping professionals doing their jobs, especially in the field of strategic warning, where the probability of a war, crisis or attack must be updated in the light of new events.

In particular, the consistent adoption of a formally correct mathematical procedure to calculate conditional probability can bring many benefits, mainly in terms of quantification and graphic display of the final assessments. It may also help managers to reduce the friction among different points of view and effectively monitor the flow of events and incoming intelligence.

Some of the problems faced in teaching, learning and actually using Bayesian statistics on the field can be overcome by means of two different kinds of tools: new cognitive techniques and information technology. In particular, it seems that the adoption of natural frequencies (like 1/4 or 1 out of 4 etc.) instead of probabilities in decimal or percentage format (0.25, 25% etc.) may greatly improve the learning mechanism (Hoffrage and Gigerenzer 1998, Sedlmeier and Gigerenzer 2001). Also decision trees proved to be effective (Kraußet al. 1998). Once the fundamentals of the theory have been acquired by the analysts, they can use a computer to automatically do the calculations.

References

1. B De Finetti, *Probability, Induction and Statistics*, (John Wiley & Sons Ltd, 1972).
2. B De Finetti, *Theory of Probability*, (John Wiley & Sons Ltd, 1974).
3. DM Eddy, „Probabilistic reasoning in clinical medicine: Problems and opportunities”, in Kahneman D, Slovic P and Tversky A (Eds.), *Judgment under uncertainty: Heuristics and biases*, (Cambridge (UK): (Cambridge University Press, 1982), pp. 249-267.
4. C Fisk, „The Sino-Soviet border dispute: A comparison of the conventional and Bayesian methods for intelligence warning”, in *Studies in Intelligence*, 16(2), 1972, pp. 53-62.
5. RJ Heuer, *Psychology of Intelligence Analysis*, (Center for the Study of Intelligence, Central Intelligence Agency, 1999).
6. U Hoffrage, Gigerenzer G, „Using natural frequencies to improve diagnostic inferences”, in *Acad Med*, 73(5), 1998, pp. 538-40, May.
7. D Kahneman and Tversky A, „Subjective probability: A judgment of representativeness”, in *Cognitive Psychology*, 1972, 3, pp. 430-454.

8. S Krauß, Martignon L and Hoffrage U, „Simplifying Bayesian Inference", in *Proceedings of the Conference on Model-Based Reasoning in Scientific Discovery*, 1998.
9. M Schield and Burnham TVV, „Von Mises' Frequentist Approach to Probability", in *Proceedings of the Section on Statistical Education of the American Statistical Association*, 2008, pp. 2187-2194.
10. N Schweitzer, „Bayesian Analysis for Intelligence: Some Focus on the Middle East", in *Studies in Intelligence*, 1976, 20(2), pp. 31-44.
11. P Sedlmeier and Gigerenzer G. „Teaching Bayesian reasoning in less than two hours", in *J ExpPsychol Gen*, 2001, Sep, 130(3), pp. 380-400.
12. A Tversky and Kahneman D, "Belief in the law of small numbers", *Psychological Bulletin*, American Psychological Association, 1971, 76(2), pp. 105-110.
13. J Zlotnick, Bayes Theorem for Intelligence Analysis, in *Proceedings of the Conference on the Diagnostic Process*, (Ann Arbor, Michigan (USA), 18 June 1970).

A New Challenge in Data Analysis: The Big Data Phenomenon

Marcel FOCA[*]
Ionel NIȚU[*]

Abstract

In this paper I did not approach the "Big Data" concept from a perspective of storing large data volumes or cloud computing, but from the perspective of managing/processing large data volumes and their diversity (structured/ unstructured, public/confidential, extremely different subject areas, various sources: TV, radio, photo-video, GIS[1] etc.).

I treated the Big Data phenomenon taking into account all the challenges this poses to data analysis. We are considering a number of implications of this phenomenon, such as:

- the exponential growth of stored data (public or confidential) and their diversity;

- the increased difficulties in processing data for generating actionable information (considering the need to make decisions in real time);

- the security/confidentiality issues arising from the Big Data phenomenon;

- a trend to replace data analysis by extrapolation (based on data samples), with the analysis of the entire data.

If the structured data (which include databases with aggregation, searching and processing rules) are relatively easy to integrate, data analysis must be extended to include unstructured data (in even greater numbers, at least if we consider those we can find on the Internet).

This is a change in the paradigm of the world of information technology and intelligence, one we must fully understand in order to be able to adapt to it.

We must be smart, prospective and pro-active, we must anticipate change instead of just reacting to stimuli.

Keywords: Big Data, analysis, intelligence, internet, GIS, geospatial

Instead of introduction – three short examples

● We cannot know the exact accuracy of an opinion poll for predicting the winner of the Eurovision singing competition (May 2013) – it must have been based on certain subjective factors,

[*] MBA, Intergraph Computer Services, Romania
[*] PhD, assistant professor, Intergraph Computer Services, Romania

such as sample selection, the responders' availability to provide answers and it would certainly not have been able to take into account any of the background support agreements between the various peoples, which always happen at the Eurovision.

Nevertheless, Denmark's victory was foretold – with a rather high degree of precision – by an IT researcher who used a Big Data analysis software.[2]

● Using the specific Big Data analysis methods of a certain search engine, researchers were able to anticipate, rather accurately, the flu propagation model for the H1N1 virus[3].

● During the American elections (November 2012), a website predicted that Obama will be re-elected[4], by using a data model which correlates information (by multiple categories) from all election results in the USA from 1940 until present times.

These three examples are using different logics, but they all show that the analysis can be digitalized at least up to a certain point.

To these three examples we will furthermore add new analysis parameters, all specific to the Big Data phenomenon, namely: volume, diversity and exponential growth ("tsunami").

The volume of internet data is growing exponentially

● At the end of 2011, the number of internet users was estimated to 2.1 billion, and it will rapidly reach the benchmark of 50% of the world's population. The number of existing websites was estimated (at the end of 2011) to 555 million, not taking into account personal pages.

In only a few months, this number exceeded 620 million[5], which means a growth rate of around 7 million sites/month.

It seems that this trend is here to stay, because the same NetCraft estimated a count of around 101 million websites, in 2006.

This means that 454 million new websites appeared in the span of 5 years, which again averages around 7 million sites per month.

Considering that 2-3 new websites appear every second, creating such an inventory has become a daunting task.

● As for the volume of data and information circulating around the Internet, things get even more complicated, because we must now include e-mail, forums etc., which tend to replace classical forms of communication (according to Osterman Research, around 116 billion messages are sent and received each day, which means around 20 messages per person every day[6]).

● We won't even take into account the fact the Internet means more than just officially accessible pages: there is also the deep web, a facet of the virtual world which cannot be measured.

● The volume of data generated on a daily basis doubles every 40 months, which means that more data are generated every second than the total data existing on the Internet 20 years ago.[7] Around 90% of the current data on the Internet was generated only in the past 2 years.

If we consider also the statistics regarding the growth of telecommunication data – (a 1.000 times growth in the past 20 years –according to the Orange company), we have an image of how complex and bubbly this field has become.[8]

● In Romania, at the beginning of this year, the number of Internet users was estimated to 9.6 million, but any attempt to inventory the number of websites is distorted by the variety of the domain names used (.ro, .com, .org, .edu, .eu etc.).[9]

Since we are talking about .ro domains, in 2006 there were around 120.000 web pages, and currently that number is estimated to reach over 600.000[10].

Even if at a slower pace, the growth is obvious and it will probably pick up the pace once the governments will increase the number and quality of electronic services for the population.

● Big Data means more than just the Internet, it also means billion of data accumulated in their own data bases (let's only imagine the volume of information accumulated by American agencies such as NASA or the NSA, or the historical data archived with the NGA, mainly as images or satellite videos).

After terabytes, we had to invent larger units of measurement for data volumes (peta, exa, zeta).

Diversity creates new challenges

● Smartphones, sensors (whether terrestrial, aquatic or on satellites), video cameras, smart meters and other connected devices generate huge volumes of data added to the already gigantic stock of data from traditional sources.

At first glance, all these new data can be a gold mine for data analysis, which can check their authenticity according to the classical rule of finding at least two or three other sources of information, but all these will make things complicate, even more.[11]

We live in an age where UAVs and drones replace airplanes, where self-driven cars and smart highways are about to become reality.

The volume of data collected by one drone in a day, that alone, requires weeks of analysis and interpretation.

Therefore, we have completely different things that could be corroborated and integrated inside Big Data.

Satellite information, together with database and sensor information (biochemical sensors, radars etc.) are nowadays integrated in real time and delivered to mobile devices, no matter how large the volume of the processed data.

Even the processing can be outsourced from the cloud, so we no longer need to have in-house analysis capabilities.

● In their book *Big Data: A revolution that will transform the way we live*, Viktor Mayer-Schönberger and Kenneth Cukiernethink that many aspects of our daily life can be digitized and transformed into data, and soon everything may become digitized. From food to political preferences, from professional history to hobbies and vices, attitude, character, skills, strong or weak points – everything could become part of one giant database. Obviously, to the extent that each of us is a part of an organization, region/country, culture/religion etc., the Big Data phenomenon can include that as well.[12]

In the authors' opinion, the first and foremost advantage will be awarded by scientific researches. Here, the most difficult part is collecting and selecting data within the limits of specified resources (involving time or money). And some social research methods, such as opinion polls, could be replaced by Big Data analysis.

The authors claim that, if we store all data of a certain domain, we can obtain a huge volume of information that we can use later on for research in a new and more effective manner.

"Instead of formulating hypotheses and then testing them through experiments and polls in small groups, which is a classical but error-prone procedure, scientists will turn to the advantages of Big Data: high performance, high-precision and high-power algorithms, who will scan gigantic quantities of already gathered data to quickly extract the existing trends."[13]

This is the positive side of Big Data.

Assuming that a large part of our lives will move to the Internet and/or to other data bases, how much of what we do, intend to do, think or feel is protected?

"Perhaps we don't mind other people knowing what products we use to wash the floors, or even our diseases, but Big Data won't stop at this. At a large scale, Big Data could mean what we already see at a small scale: that we may know a lot, an unpleasantly huge number of things about a person only from data gathered from the non-conspicuous, daily monitoring of absolutely prosaic and routine activities, from the basic biological ones –such as walking –to social contacts. CCTV camera may analyze for instance the way we walk and people may draw conclusions regarding not just our health but may go as far as to delve into our intimacy."[14]

How do we cope with an information tsunami?

● Considering all the above, a first challenge is generated by the fact that by now it is no longer an issue of generating the data/information we need, but how to eliminate the ones we don't need.

Since many data on the Internet cannot be dated or certified, as they are anonymous and/or false, gathering data will become less and less important and the focus will switch to searching for the authentic, correct and relevant data in this ocean of information. Until we get there we cannot talk about data processing and analysis.

At the same time, we are witnessing a change in the relevance or impact of the Big Data phenomenon.

Facebook and Twitter are becoming non-state actors, increasingly relevant on the international stage, influencing opinions and causing people to take actions ("Arabian spring", the "twitter revolution" in Moldova).

Bloggers seem to become the new journalists and opinion makers, and the Internet tends to replace the classical media. We already have radios and television channels or publications which exist only on the Internet.

● All over the world, these globalization realities are overwritten by the need to make decisions in real time, which involves ever-growing and ever-more refined analysis capabilities.

Data analysis will grow in importance and it will require evolved software (allowing for relevant searches in the Big Data and making correlations between information).

Future analysts will probably have to have more than just processing and thinking skills (critical or creative thinking), they will also need IT skills.

Big Data analysis is already considered as a new analysis category, combining statistical analysis with the ability to look for and correlate unstructured/disparate information.

Some IT companies talk about automatic analysis systems (Big Data Analytics), "allowing business leaders to analyze massive data volumes shared by their employees and discover trends in their fields of activity which they can use to build more productive working environments and minimize efforts".[15]

We don't believe that data analysis can be rendered fully automatically. Quite on the contrary, the human factor involved in processing information is probably even more important than having the sum of information.

This is the reason why Intergraph Computer Services supported and promoted the process for introducing the "information analyst" job in the Romanian Job Classification (which they succeeded in March 2012) and for creating the related occupational standards (approved by the National Qualifications Authority in April 2013).

But analysts must claim an even more important role in the institutional landscape and beyond (for instance, in the intelligence cycle), they target society itself.

It is in fact a change in paradigm which renders the old saying "information is power" a mere relic of the past century.

Knowledge is power, and knowledge is provided by analysis and analysts

The billions of existing data are only useful to those who can search, sort through and correlate them, to those who can understand and use them.

This requires automating the analysis.

● Here are several examples of what an automated analysis can do for large data volumes:

- the FBI approached the Big Data in 1999, when it launched the digital fingerprint recording system, now holding fingerprints of over 55 million people in its data base.

The response time of this software for the identification of a set of fingerprints in a subset of 2 million of potentially dangerous people was only 2 hours; and for usual cases (mainly civilian cases) the response time was 24 hours.

In 2011 the system was upgraded and now the response times are: 10 minutes for urgent queries; between 15 and 30 minutes for normal queries; maximum 120 hours routine checks.[16]

- In Boston, in less than 24 hours after the explosions, the FBI processed around 10 terabytes of information: phone calls, text messages, photos, videos and social media. They used facial recognition technologies to match faces in photos and faces recorded in databases for driver's licenses, passports, visas etc.

Although 10 TB is nothing but a drop in the ocean of petabytes the FBI usually works with, the agency was able to produce very valuable information in a very short time, and thus capture the criminals.[17]

As for the terrorist attempts in Boston, paradoxically, FBI didn't think Tamerlan Tsarnaev was a potential terrorist because Aeroflot got his name wrong on the boarding list (so the passenger list that the FBI had did not match the data base).[18]

Of course, the ideal is to prevent any terrorist actions. This requires real time decisions.

● Since we are discussing Big Data and changes, we can add that the need for real time decisions often implies real time analysis, with interactive IT software that can be updated in real time.

We are talking about concepts such as on-line dispatch centers and command & control decision systems (C2), where the role of GIS information and geospatial analysis makes the difference.

In the GIS world it was always about Big Data, given the enormous data volumes and diversities (also the diverse sources of information) and the need to make quick decisions.

"Geospatial Data has always been Big Data. Now Big Data Analytics for geospatial data is available to allow users to analyze massive volumes of geospatial data. Petabyte archives for remotely sensed geodata were being planned in the 1980s, and growth has met expectations. Add to this the ever increasing volume and reliability of real time sensor observations, the need for high performance, big data analytics for modeling and simulation of geospatially enabled content is greater than ever."[19]

The greatest challenge for GIS is standardization for interoperability. Standardization of geospatial information facilitates real time data processing, cooperation and exchange.

In order to make the information "come to life" (updated in real time), we need workflows to carry the information through software facilitating real time decisions.

The difference between planting a bomb on a children's bus in Afghanistan and precisely identifying the location of Osama Bin Laden's hideout, or the difference between the annihilation of the Chechen leader Dudaev, after a phone call, and the bombing by mistake of China's Embassy in Belgrade during the Serbian conflict is in the precision of the geospatial information.

The ability of making real time decisions in a world where the analyzed environment evolves rapidly will make a difference. Information quality and precision will be vital, and the difference will be made by analysts.

Instead of conclusions

● A study made at the beginning of this year (including IT managers and experts) has shown that:

- over 60% of the responders think that Big Data will be a strategic priority for their companies, because it will help increase competitiveness and decision-making;
- over 70% intend to make sure their Big Data plans include data from non-conventional "intelligent devices" (digital sensors, intelligent meters, video and others), 30% are already collecting unstructured data, such as the video feeds;
- around 40% can analyze data in real time, then use and eliminate it;
- 27% claim that data security and risk management are a major concern regarding Big Data.[20]

● The Big Data concept is ever more present in our day-to-day lives. It is associated with clouding, and our lives (professional, personal or commercial) are slowly but surely switching over to the Internet.

We should also mention the latest trends in electronic voting and digital coins, that leads to new frontiers after Germany officially recognized the existence of the "bitcoin". The IT arena is becoming more important among other commercial markets, these companies registering higher growths in the financial markets.

Some analysts are even talking about the higher financial power of companies compared to countries, like Apple's market capitalization being higher than many countries' GDP.

● Confidentiality issues (that is, intimacy risks) meet security issues, in an age where the greatest challenge – the cyber threats – target the very essence of Big Data. The latest trends show us an increase in the likelihood and impact these threats have on security and business environments.

Let's not forget that smartphones collect data about our private lives without asking for our approval. Until proven otherwise, we can go on thinking that this data did not get into the hands of evil-minded people, although it can feel uncomfortable knowing that certain intimate aspects of our lives are revealed to others.

In the same way, social media networks collect personal data, although – to the best of our knowledge – they do not obey the laws of the countries where their members/users are located (national accreditation for personal data operators). After the PRISM scandal it is possible that security and confidentiality protection matters will be brought to public attention, to keep Big Data from being seen more as an intrusive phenomenon in our lives.

● Information analysis is more and more important, as it helps decision-making in real time, but it need to be automated to be effective, because an analogue (manual) analysis on large data volumes is completely unfeasible.

Without analysis, Big Data can provide incredible quantities of punctual data about the entities we are interested in. Quantity is not quality, however, and sometimes having access to too much can mean having access to nothing at all.

To understand an entity in the whole and in its context (in all its complexity) we need a new type of analysis, based on algorithms and indexes applicable on unstructured data, that is, on mathematics.

The greatest challenge is not integrating databases full of structured data (which is being done slowly, but it is being done nevertheless), but to integrate unstructured data, this growing at faster rates by the minute.

● One of the greatest challenges will be the specialization of human resources.

Romania does not lack people talented in IT and mathematics, as proven by the many awards gained at international contests. The problem is we don't seem to be able to use this important resource for increasing our country's competitiveness worldwide, and these young people are not to blame for this.

We feel more than ever the need to support the IT field, which seems to have turned into the new grounds of economic competition all over the world. If Romania lost the big prizes in other areas, maybe in the IT area and in particular in the Big Data Analysis area (which requires new thinking patterns, creativity and innovation) we stand a chance to make it up to the rest of the EU.

In the end worth to mention that big governmental IT projects seem to be lost somewhere (abandon? stand-by?): e-Romania, the law of national registries, electronic ID cards, governmental intranet, internet for all schools. It might not be too late to have a Big Data Analysis division at the central government level with a double role: to process and to analyze Big Data information (as a support for the strategic development policies) and to monitor the implementation of the strategic IT decisions (to make Romania passing over the “IT consumer” phase).

References

[1] Geographic Information System.

[2] Steve McCaskill, *Eurovision Big Data Researchers Predict Victory For Denmark*, available online at http://www.techweekeurope.co.uk/news/eurovision-big-data-microsoft-research-116561 (accessed on August 28, 2013)

[3] Mircea Sarbu, *Big data şi cutia Pandorei*, available online at http://www.businessmagazin.ro/opinii/big-data-si-cutia-pandorei-10658431 (accessed on August 28, 2013).

[4] http://www.tableausoftware.com/public/gallery/us-election-predictions (accessed on August 28, 2013).

[5] According to www.NetCraft.com

[6] http://www.agora.ro/stire/ibm-ofera-cea-mai-avansata-experienta-de-socializare-din-industrie-pentru-companii (accessed on August 28, 2013).

[7] http://www.bigdata.ro/big-data/ (accessed on August 28, 2013).

[8] Valentina Crisan, *Aproape totul despre Big Data @BigDataWeek*, available online at http://www.eurocloud.ro/big-data-week/#.UZjIcj4mH3Q (accessed on August 28, 2013).

[9] Cristina Negraru, *Internet Word Stats: In Romania sunt 9,6 milioane utilizatori de internet*, available online at http://www.wall-street.ro/articol/IT-C-Tehnologie/142316/internet-world-stats-in-romania-sunt-9-6-milioane-de-utilizatori-de-internet.html (accessed on August 28, 2013).

[10] http://www.123wp.ro/cate-domenii-ro-active-exista-pana-acum/(accessed on August 28, 2013).

[11] http://ittrends.ro/2013/04/big-data-potential-imens-prioritate-ridicata/ (accessed on August 28, 2013).

[12] Mihaela Stănescu, *Big Data – revoluţia care ne va schimba viaţa*, available online at http://www.descopera.ro/cultura/10735565-big-data-revolutia-care-ne-va-schimba-viata (accessed on August 28, 2013).

[13] *Ibid*.

[14] *Ibid*.

[15] Radu Ghitulescu, *IBM prezintă noi servicii şi produse software Big Data analytics*, available online at http://www.marketwatch.ro/articol/12383/IBM _prezinta_noi_servicii_si_produse_software_Big_Data_analytics, (accessed on August 28, 2013).

[16] Alex Olesker, *Big Data Figts Crime: The FBI's Next Generation Identification*, available online at http://ctovision.com/2011/12/big-data-fights-crime-the-fbis-next-generation-identification/(accessed on August 28, 2013).

[17] Sonny Singh, *How Big Data is Helping Catch Criminals*, available online at .http://o-www.emulex.com/blogs/labs/2013/05/14/big-data-helping-catch-criminals/ (accessed on August 28, 2013).

[18] Bill Wise, *Big Data's Usability Problem*, available online at http://allthingsd.com/20130423/big-datas-usability-problem/ (accessed on August 28, 2013).

[19] George Percivall, *Big Processing of Geospatial Data*, article available online at http://www.opengeospatial.org/blog/1866 (accessed on August 28, 2013).

[20] http://ittrends.ro/2013/04/big-data-potential-imens-prioritate-ridicata/ (accessed on August 28, 2013).

Decision Theory Applications in Intelligence

Maria-Cristina MURARU[*]

Abstract

The intelligence field is based on the idea of rational decision-making, which relies on the logical mixture between criteria, options and the consequences they are likely to create.

Beyond the intelligence organizations and process-specific means and methods, one can observe significant similarities with the Decision Theory domain, especially in the manner of thinking. In other words, both fields apply the same Minimax principle of gaining the maximum benefits with minimum risk.

To this end, the present paper proposes to prove the utility of applying Decision Theory-specific concepts and methods in the intelligence area, particularly at the analytical level. Furthermore, we shall describe the general methodology, one that grants the possibility of maximizing the utility of the decision-making, in terms of uncertainty, options and multiple criteria.

Keywords: decision, (un)certainty, utility, criterion, alternative.

Introduction in decision theory

Our daily activity is a sum of decisions: we are granted access to a variety of alternatives whose utilities we are aware of, we also know the alternatives' costs and we create our own set of criteria to evaluate these possible choices.

The modern decision theory has developed since the middle of the 20th century through contributions from several academic disciplines. It is an interdisciplinary domain to which statisticians, economists, psychologists and computer scientists add their expertise. In this domain, everyday terms such as risk, uncertainty and ignorance are used as technical terms with precise meanings[1]. In the decision under risk the decision-maker knows the probability of the possible outcomes, whereas in the decision under ignorance the probabilities are either unknown or non-existent. Uncertainty is either used as a synonym for ignorance, or as a broader term referring to both risk and ignorance. Although decisions under ignorance are based on less information than decisions under risk, it does not follow that decisions under ignorance must therefore be more difficult to make[2].

[*] Intelligence expert, Romanian Intelligence Service, Romania

Any decision process is described by a series of steps taken:

- Defining the problem;
- Developing a set of criteria;
- Data mining;
- Using found data in developing possible alternatives;
- Assign each alternative a probability degree of materializing;
- Assign each criterion an importance coefficient;
- Comparing the options using their probabilities;
- Choosing the best option, after consulting the list of criteria and their coefficients;
- Applying the decision[3].

Although the previously-described decision process appears to be simple, there are certain factors that can raise questions. For instance, the most difficult aspect in the process is developing the set of criteria and identifying the information actually required to simplify the entire system.

Furthermore, despite the fact that it is more probable to choose the best alternative, the more the criteria, the more amount of time needed to decide which alternative is best suited for the objective. Moreover, when assigning coefficients to criteria, we deal with time consumption, leading to a bigger time constraint on the decision process. Also, the members of a decision-making team have different sets of values and principles, experience, expertise and education, resulting in a variety of opinions on the same subject.

Another obstacle resides in the small amount of information about the possible consequences of each alternative; the degree of uncertainty is thus significantly amplified.

Normative *versus* descriptive

Decision theorists, experts per se in their own fields, agree on a set of concepts that clearly distinguish between *descriptive* and *normative* decision theory.

The main difference between the two is that while descriptive decision theory seeks to explain and predict how people actually make decisions, the normative theories yield methodologies and rules on the rational course of action. It is also self-understood that the descriptive decision theory implies rational thinking, having avoided the use of highly advanced mathematic concepts such as Bayesian probabilities or differential equations.

Furthermore, considering Laurence J. Peter's motto: "some problems are so complex that you have to be highly intelligent and well informed just to be undecided about them" and the variety of today's data sources we can state that applying rational decision theory is highly improbable. Rational decision theory implies an extensive use of state-of-the-art of mathematical models and algorithms, and also an individual well acquainted with these concepts.

The present paper will further describe three major decision-making processes that have been and are being currently applied in today's intelligence craft.

Decision and intelligence cycle

In order to understand why decision is the central core of the intelligence process, especially at the analytical level, it is important to describe the way the diverse entities of the intelligence community contribute to the decision-making process.

The best way to describe the importance of decisions is to explain every step in the intelligence cycle and their specific decision[4].

1. Planning and direction: intelligence consumers or policy-makers decide on the needed intelligence product to support decision-making. Thus the intelligence cycle is based on a priori decision.

2. Collection. When working from clear requirement, the intelligence community begins to gather raw data for analysis. Specific information is identified for collection and certain sources and means are consulted. Thus it is decided what is needed and how it will be obtained.

3. Processing. This step refines raw data to usable information for analysis. It implies expertise in decoding signals, understanding satellite imagery, multilingual translation etc. Therefore, the decision-making process appears in terms of choosing the best-suited experts for data processing.

4. Analysis. During this stage, experts evaluate information, drawing conclusions from current reports, but also from historical

knowledge on the problem. The art of analysis often requires deciding that more information is needed or that new sources need to be consulted in order to get a complete view on the requirement's objective. In other words, analysis is all about choosing, therefore influencing the intelligence cycle's decision-making process.

5. Dissemination. During this step, the intelligence product is presented to the decision makers. There are cases when the decision makers request further monitoring on the analyzed matter or, worst case scenario, the entire product must be rethought, restarting, thus, the entire cycle.

We can draw the conclusion that the „decision" concept is a constant presence in the intelligence community's activity and also its main driver, especially in its most acclaimed component: analysis.

Decision-making and analysts

Intelligence analysts are required to identify the likely — and unlikely — consequences of alternative courses of action for specific, real-time problems. With time constraints and potentially critical consequences, analysts must "sail through the uncertainty sea" of the specific task, providing a best estimate of what is likely to happen, estimating the probability of different outcomes from the best estimate. In each case, there is an interest to work through the logic of a situation to ascertain what might be done to alter or to facilitate particular outcomes. Keeping the intelligence assessment open to the prospects of a discontinuous change is especially important because the past is not necessarily a predictor of the future[5].

Also, everyday analysts make significant decisions involving uncertainty in areas in which they are not experts. Moreover, credible information about uncertainty is available, although the problem is how efficient is the decision process after including this data in the cognitive system. Also, research has taught us that people are error prone when working with probability. On the other hand, the advantage of uncertainty estimates or probabilities is directly proportional with the manner of expressing them and the mathematical skills of the user. In other words, it is critical that the way of expressing probabilities be compatible with both the analyst and the task required to be completed.

When involved in solving a task, an analyst must choose from a set of alternatives, after having acknowledged their probable consequences. In theory or under laboratory-conditions, a rational person decides and chooses the optimal solution after thoroughly considering each and every alternative. Experts in economics, social sciences and mathematics have studied the behaviors of those having to decide. Their conclusions have been common: although information is the core of the decision-making process, the decider's experience, preferences and way of thinking have been proven to be crucial factors. Also, when conducting experiments, the experts indicated that when dealing with uncertainty, people tend to choose the alternative with the highest probability of materializing[6].

The intelligence cycle is filled with a number of high-stakes decision points: for instance, when planning, the analyst must decide fast whether the indicators are well-suited for the upcoming process. During the collection stage, the analyst will also evaluate sources, finally deciding if the information they provide is usable, toxic, sufficient or just plain white noise.

Decision-making processes and their impact on intelligence analysis

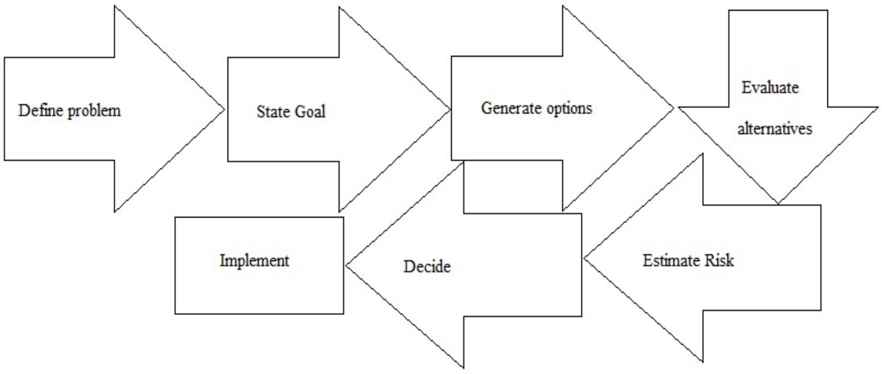
The past 50 years of intelligence analysis has taught the community that there are three major types of decision-making: traditional, naturalistic and adaptive.

➢ **The traditional process** yields to describe clear rules that analysts should follow when choosing between several alternatives. This type of process is based especially on the idea of rationality and the maximization of the utility, whilst taking minimum risks, or the so-called Minimax principle. The rational component of this framework states that analysts will always use a logical, robust process when taking a decision.

Also, this kind of process is a result of years of applying and testing strategies and methods, thus testing and continuously improving the methodologies. Effective methods consist of algorithms in decision making that are taught to junior or even trainee analysts for application in their activity.

However, years of experience have also proven that although analysts are properly trained in what we call the traditional decision-making, there are chances that these methods are not always feasible in real situations. A wide range of algorithms connected to the traditional process have been applied: Bayesian analysis, Sleipnir[7], the Electre Method[8]. As previously stated, this kind of strategies and methods will require a highly trained professional with both mathematical and analytical skills.

In other words, the traditional process is a sum of methods that simultaneously generate and evaluate options, after assuming that the analyst is rational and constant in evaluating similar situations.



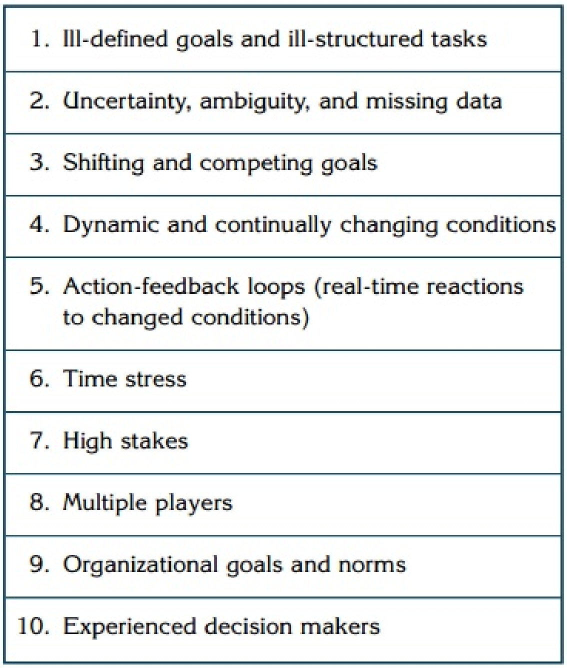
The traditional decision-making process

As is observed, the traditional decision consists of six clear and rigorous steps; the stages bring in the process just a unilateral influence, existing, thus, the risk of making errors although the method is, in theory, infallible.

➢ **The naturalistic process**, described by Gary A. Klein and his colleagues in the highly acclaimed study “Decision Making in Action: Models and Methods”[9], describes the manner in which individuals use their experience when deciding. This type of process is based on the highly intuitive component of the decisions that happen in real time situations. The naturalistic perspective intuitively creates decision-making models after evaluating the way experts develop effective strategies. This category of models can be trained, developed and used in situations where the traditional ones do not succeed.

Furthermore, naturalistic strategies are under less control and rigor than the traditional type, resulting in an increase in what we call “decision-making speed”. At the moment, there are a series of intuitive methods of analysis that are successfully used: scenario development, the Devil’s advocate and red teaming.

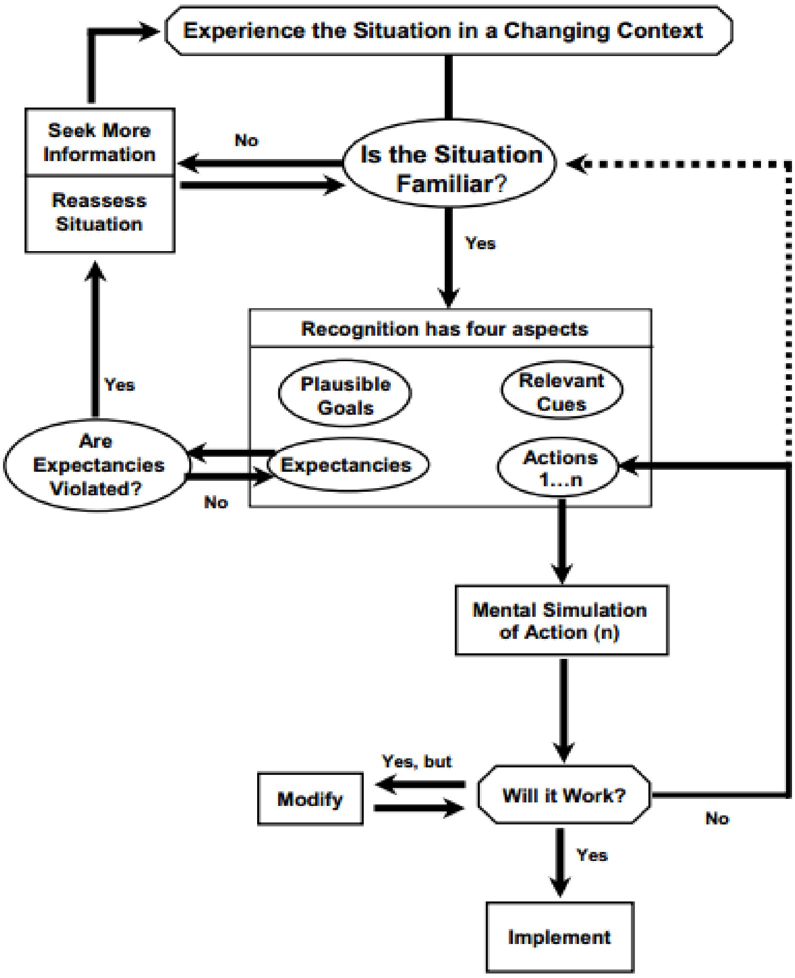
Researchers in this field have identified ten features of this manner of decision-making:



1. Ill-defined goals and ill-structured tasks
2. Uncertainty, ambiguity, and missing data
3. Shifting and competing goals
4. Dynamic and continually changing conditions
5. Action-feedback loops (real-time reactions to changed conditions)
6. Time stress
7. High stakes
8. Multiple players
9. Organizational goals and norms
10. Experienced decision makers

Klein’s characteristics of the naturalistic decision-making process[10]

The same team of researchers established a “standard” model that describes the intuitive, naturalistic decision-making process.


Experience the Situation in a Changing Context
Seek More Information
Reassess Situation
No
Is the Situation Familiar?
Yes
Recognition has four aspects
Plausible Goals
Relevant Cues
Expectancies
Actions 1...n
Yes
Are Expectancies Violated?
No
Mental Simulation of Action (n)
Yes, but
Modify
Will it Work?
No
Yes
Implement

Klein's „Model of recognition-primed decision making"

To sum up the upper image[11], when applying a naturalistic decision process, people actually use their past experience in order to establish the best course of action. Unlike the traditional process, the naturalistic type learns directly from experts' responses to situations, and does not apply a standard, "stencil"-method on a case or task. The "model" can be applied at any given point in the analysis cycle, directly depending on the analyst's experience, time constraints, personal expectations, principles and values. It is also important to state that every analyst will reach a different result in applying this decision-making process, thus differences of opinion may appear when working as part of a team.

➢ **The adaptive decision-making process** combines the prior two categories, resulting in a flexibility in applying standard methods and certain rigor in the art of analysis.

In their position as decision-makers and in a work environment described by time constraints, analysts are very often confronted with the need to resort to intuition and fast decisions. However, they are also confronted with the pressure of performing analysis in a scientific way. In other terms, not only analysis is both an art and a science, but also its decision process is a mixture of the two apparently disjunctive concepts.

Future directions of decision theory applications in intelligence

The decision-making process is one best described by the term “complexity”, often implying a significant mixture of uncertainty and risk-taking. When being applied in the intelligence field, decision-making is a continuum aspect, involving everyone, from data collectors, to analysts and policy-makers. It is therefore crucial that training courses for analysts include teaching notions regarding decision theory and its processes.

Intelligence analysis, like any other active field, has a highly unpredictable future in terms of method and human resources. Also, considering today’s trend in exploring the cognitive layers of judgment and decision, one can see the opportunities in applying certain principles of what we call “neuro-economics”[12]. This new science seeks to explain and describe the human decision process and its ability to process a variety of alternatives, further deciding the optimal course of actions. In other words, it uses cut-edge research such as brain imaging and genetic mapping in order to offer a plus of knowledge and understanding the way people make decisions[13]. It is therefore crucial for the intelligence community not only to continuously seek to understand and enhance its decision processes at any given level, but also to be connected to the latest research in decision theory and its applications in similar interdisciplinary fields.

References

[1] Sven Ove Hansson, "Decision Theory. A brief introduction", accessed on 30 July 2013 at http://home.abe.kth.se/~soh/decisiontheory.pdf

[2] Martin Peterson, *An introduction to Decision Theory*, (Cambridge: Cambridge University Press 2011), pp. 4-10.

[3] Ion Dobre, *Decision Theory* Course – Faculty of Cybernetics, Statistics and Economic Informatics, (ASE Bucharest, 2010).

[4] Steven W. Peterson, *US Intelligence Support to Decision Making* accessed 11 August 2013 at http://programs.wcfia.harvard.edu/files/fellows/files/peterson.pdf

[5] Bruce Bueno de Mesquita, *Intelligence Analysis: Behavioral and Social Scientific Foundations* accessed on 8 August 2013 at http://www.nap.edu/openbook.php?record_id=13062&page=57

[6] Richards Heuer, *Psychology of Intelligence Analysis*, (Center for Study of Intelligence: 2013), pp. 111-161.

[7] The Sleipnir technique provides intelligence analysts working on organized crime groups with a comprehensive and transparent method to assist in developing and presenting recommendations and supporting intelligence in a concise manner. / Royal Canadian Mounted Police, "Sleipnir Version 2.0". Organised Crime Groups Capability Measurement Matrix" accessed 11 August 2013 at http://jratcliffe.net/research/sleipnir/SLEIPNIRv2_unclassified.pdf

[8] Multicriteria decision algorithm / Ion Dobre, *Decision Theory Course – Faculty of Cybernetics, Statistics and Economic Informatics*, (ASE Bucharest), 2010.

[9] Gary Klein, Judith Orasanu, *Decision Making in Action: Models and methods*, (Ablex Publishing Corporation 1993).

[10] Gary Klein, David Klinger, *Naturalistic decision-making* accessed on 6 August 2013 at http://www.au.af.mil/AU/AWC/AWCGATE/decision/nat-dm.pdf

[11] Gary Klein, *Naturalistic Decision Making*, accessed on 9 August 2013 at http://www.ise.ncsu.edu/nsf_itr/794B/papers/Klein_2008_HF_NDM.pdf

[12] Reid Hastie, Robyn M. Dawes, *Rational Choices in an Uncertain World*, (Los Angeles: Sage 2010), pp. 295-300.

[13] John Steiner, *Neuro-Economics- Convergence* accessed on 10 August 2013 at http://www.phibetaiota.net/2012/03/john-steiner-neuro-economics-convergence-recap/

Violent Extremist Risk Assessment for Intelligence Use: VERA 2 Applications and Evaluation

D. Elaine PRESSMAN[*]

Abstract

The Violent Extremist Risk Assessment Protocol (VERA-2) is discussed in terms of its applications to the intelligence community. The standardized, systematic and transparent approach of the VERA 2 can assist in enhancing the reliability and accuracy of individual-based risk assessment for intelligence use. The VERA 2 is being used on four continents including member states of the EU, North America and in the Asia-Pacific region. The tool has potential for assisting intelligence analysts with the assessment of suspected violent extremists, differentiating risk in ideologically motivated fighters returning "home" from engagement in conflict areas abroad, classifying the risk of "terrorist" detainees in prisons and detention centers, monitoring the changes in risk over time of suspected violent extremists and assessing the efficacy of violent extremist de-radicalization programs. The VERA 2 uses the structured professional judgment approach and the protocol has been demonstrated to possess several different types of validity. Its benefit to the intelligence community is in supporting analyst judgment with additional verification and enhancing the objectivity and scientific nature of intelligence analysis.

Keywords: risk assessment, terrorism, scientific-led intelligence analysis, violent extremism, individual risk analysis

Introduction

Individual acts of violent extremism have been identified as a major threat in the volatile security environment of the 21st Century. In comments to The Senate Select Committee on Intelligence on January 29, 2014, James R. Clapper, the U.S. Director of National Intelligence suggested that the present is beset by more crises and threats around the world and is more complex and dangerous than at any period in the past 50 years.[1]The Boston Marathon bombings, allegedly perpetrated by brothers Tamerlan and Dzhokhar and which killed 3 and injured more than 260 on April 15, 2013, underscores such threats.[2] The bombings also highlight the complexity of predicting these events and of assessing the individual risk of individuals for violent extremism.

Many experts consider the missed cues in the case of Tamerlan Tsarnaev, the elder brother, to be an example of intelligence failure. Tamerlan Tsarnaev had been identified as a potential threat by the

[*] Senior Fellow, Canadian Centre for Intelligence and Security Studies, NPSIA, Carleton University, Canada

Federal Security Service of the Russian Federation (FSB) two years before the attack. Information on Tamerlan is reported to have been communicated by the FSB to the United States Federal Bureau of Investigation (FBI) in March 2011 and again six months later to the CIA.[3] The FSB, the principal domestic security agency of the Russian Federation responsible for domestic surveillance, counter-intelligence and counter-terrorism, reported that Tamerlan was in contact with militant Islamist groups, that he was increasing in radicalization since 2010, and that he was planning a trip to Dagestan and Chechnya where he was likely to have contact with other militants and mujahedeen. At least one member of his family was a known follower of militant Islam. Tamerlan had a personal grievance against the U.S. government because he had demonstrated his skill as a regional (New England) boxing champion but was not permitted to participate in the national boxing championships as he was not a U.S. citizen.

These elements are known "risk indicators" for violent extremism and are included elements in the structured evaluation protocol of the VERA 2.[4] Intelligence "lapses" in individual risk analysis could well be reduced by the use of comprehensive methodologies that identify and systematically explore such risk indicators. It is not known if any formalized risk assessment protocol was actually used in Tamerlan Tsarnaev's case. It is not known what protocol was used in the FBI interview with Tamerlan. It is known that the outcome decision of this interview was flawed. Risk indicators were present and information was available from the FSB sources. The fact that the final risk decision indicated nothing "derogatory" and resulted in the case being closed is perplexing. At a minimum, follow-up re-assessments over time could have been recommended due to the dynamic nature of radicalization, and the need for the collection of additional information to complete a comprehensive evaluation. Richard Falkenrath, the former deputy commissioner of New York Police Department (NYPD) Counter terrorism remarked that "the case raises questions about the suitability of intelligence operations". He also noted that "it is an investigators worst nightmare, to have your eyes on a person, allow him to drop from your attention, and then have him carry out a terrorist attack".[5]

The Tsarnaev brothers are not the only example where the application of a standardized risk assessment approach would be of utility for intelligence investigations. Risk assessments for violent extremists can be applied to insider threats in the military as well in other government agencies. U.S. Army Major Nidal Malik Hasan killed 13 people and wounded 32 others at Fort Hood, Texas on November 5, 2009. Hasan, a serving Army psychiatrist, had been identified by the FBI for further investigation. This was due to his history of email communications with Anwar al-Awlaki, a known anti-American recruiter of terrorists also implicated in planned attacks by homegrown U.S. violent extremists. Complaints about Hasan had been received from colleagues and an instructor in the military who thought he was a "ticking time bomb". Concerns were expressed by colleagues about his anti-war rhetoric, virulent extremist comments made in his lectures, and his strong and morally indignant opposition to the war in Afghanistan. The FBI identified him as a target for investigation for risk of violent extremism but no follow-up occurred despite the substantial risk indicators that were present. No details are available about the methodology that was used for the risk assessment of Nidal Hasan or even if one was undertaken to justify the risk decision. A U.S. Senate Committee on Homeland Security and Governmental Affairs investigated the Fort Hood shootings and produced a report that indicated that the FBI had not updated its tradecraft in terms of the methods and processes that were available for investigations and analyses related to violent extremism and radicalization. The report firmly advised the FBI to ensure that all of its tradecraft is systematically examined so that flaws can be corrected prior to failures.[6] The use of systematic and relevant risk indicator assessments for violent extremism, at given time intervals could have provided the empirical evidence of Hasan's increasing radicalization and sounded the alarm to the risk of violent extremist action. This could have prevented the attack.

Other applications for the VERA 2 exist within the intelligence sector. The risk posed by individuals who leave their countries to "fight" abroad in conflict areas is one of the most serious security concerns of European and North American intelligence services. These "fighters" in Syria, Afghanistan, Pakistan, Yemen, and Somalia are often engaged in combat, and may be associated with al-Qaeda affiliated groups. Britain's security minister reported that the U.K. is "very closely" monitoring those who are seeking to travel to Syria and also monitoring them on their return due to the perceived risk they may pose to the U.K.[7] The National Coordinator for Security and Counterterrorism in the Netherlands expressed the same concern specifying that these individuals can return home "battle-hardened, further radicalized, traumatized" and more closely connected with extremist groups.[8] This "danger" was the reason provided for elevating the terrorism threat level in the Netherlands. The Canadian Intelligence and Security Service (CSIS) estimated that 130 Canadians are working abroad in support of extremist activities and involved in activities such as paramilitary operations, training in weapons and explosives, and fundraising. [9]

Although it is generally agreed that returnees may pose a risk to national security, not all returnees will represent the same risk. Differentiation in the individual risk posed by returnees is necessary to determine. Furthermore, these assessments must be transparent and defensible. The Supreme Court of Canada has ordered the Canadian Security and Intelligence Service (CSIS) to retain and be able to produce the notes and recordings that it had been accustomed to routinely destroying in identifying potential "terrorists". The ruling is intended to protect the civil liberties of terrorism suspects who want to fight the allegations. This new transparency requirement requires that any determination of risk be undertaken with as much objectivity and scientific scrutiny as possible.

Detention facilities have been developed around the world where suspected or known terrorists are confined. Some are awaiting the legal process while others are incarcerated for an indefinite period. Decisions must be made as to the continuing danger represented by these detainees. A specialized tool such as the VERA 2 is appropriate for use with these alleged terrorists. It can be used to support release decisions or to recommend continued detention in these environments and use over the past 4 years in the prison setting with convicted terrorists has yielded positive results. The VERA 2 use has assisted in classification decisions (severity of the offender), placement decisions (level of security), program decisions, progression decisions (movement of inmate to a lower or higher security status) and results from the protocol have contributed to the regular reviews of serious offenders.[10] Many extremist detainees are still confined in long-term detention in Guantanamo Bay, in the Philippines, in post-war detention camps in Sri Lanka and elsewhere. Some require an assessment before release. The VERA 2 is poised to be used for this task and also for determining the efficacy of de-radicalization initiatives related to individuals and programs. This would be achieved by establishing baselines at the onset of programs with measurements of change or lack of same observed in relation to the intervention provided.

Heuer pointed out that active intelligence analysts should be concerned about "how they make judgments and reach conclusions, not just about the judgments and conclusions themselves"[11]. With the increasing demands for such transparency and accuracy, the methodology used to obtain intelligence products should be as objective and standardized as possible. The VERA 2 which uses an established and recognized risk assessment methodology is useful where uncertainty and ambiguity is ubiquitous and a scientific-led approach to intelligence is desired.

The VERA 2 – Violent Extremist Risk Assessment Approach

The VERA 2 (an acronym for "violent extremism risk assessment, revised version 2) is a structured professional judgment (SPJ) risk assessment protocol. The VERA was first introduced in 2009 as a consultative tool.[12] The protocol was revised in 2010 as the VERA 2 after an extended period of use in a high security prison system with convicted terrorists. In addition to use in the correctional system with terrorists, feedback from experts in counter-terrorism, risk assessment methodology, forensic psychology, and law enforcement operations was solicited. Recommendations were integrated into the revision. The VERA was one of the first risk assessment protocols specifically developed for use with violent political extremists and terrorists and its successor, the VERA 2 is currently in use by experts in intelligence, security and by specialists in correctional facilities on four continent including Europe, Asia, North America and Australia.[13]It is available in three languages.

The VERA was developed to meet the need identified for a risk assessment tool with indicators specific to violent extremism and terrorism. The indicators used in previously available risk assessment tools for unlawful violence were noted to differ significantly from those known to be appropriate for violent extremists. Terrorists, as most experts have found, are essentially "normal" functioning persons.[14]They are often educated or skilled, employed in professions or employable. They have families and friends and are often respected members of their communities. They are capable of normal social relationships and generally function adequately within society. They can demonstrate empathy for others but this may be a selective empathy related to their "in-group" and not their perceived enemies. These indicators differ from ordinary violent offenders who instead often exhibit behavioral problems such as impulsivity, have personality disorders, may be psychopathic, have histories of mental illness, school failure, childhood abuse, and often have a notable history of early violence. Ordinary violent offenders often have criminogenic needs such as alcohol addiction, drug addiction and/or uncontrollable urges.[15] Terrorist performance on regular risk assessment tools result in inaccurate low risk ratings due to the minimal relevance of most the indicators used.

The VERA 2 consists of 31 indicators which have an empirical grounding[16] and these indicators have been justified for inclusion based on the established terrorism and violent extremism knowledge base.[17] The included indicators are all measurable on the basis of pre-defined levels. A low rating on a risk indicator reflects less risk than a moderate or high rating. The indicators are divided into five sectors: (1) *attitudes, beliefs (ideology)* comprising 7 indicators related to elements such as the commitment to violence to further ideological goals, grievances, perceived injustices, identity issues; (2) *context and intention* comprising 7 indicators related to such elements as personal contact with violent extremists, seeking out extremist materials, intention to plan acts of violence; (3) *history and capacity* comprising six indicators such as those related to past experiences with violence, training with weapons and explosives, access to funds and other resources to support violent extremist acts; (4) *motivation and commitment* comprising 6 indicators that can generate a motivational mapping of the impact of drivers such as ideology, excitement and adventure, group commitment, moral imperative and/or criminal opportunism; (5) protective elements comprising six risk mitigating indicators that include but are not restricted to elements such as family influences, community attitudes, change in view of the enemy, other observed attitudinal changes. Ratings for each indicator are based on behavioral evidence from multiple sources. Available information is restructured according to the indicators. The final risk judgment is made after consideration of all the evidence, data and ratings produced and this is not determined in an additive manner. The overall risk decision is the result of professional judgment based on all the known information and the knowledge generated via the ratings.

Training is required for users of the VERA 2 tool. This is consistent with other structured professional judgment risk assessment tools. The training is intended to calibrate the ratings of different users against a standard, to familiarize users with the definitions and interpretation of the indicators and to ensure users gain experience with the approach. The VERA 2 does not predict who will become a terrorist from a general population. It cannot predict with certainty who will engage in acts of violent extremism. It can provide a systematic analysis of risk of those who are persons of interest or suspected of violent extremism activities through the use of relevant and transparent risk indicators for violent extremism. A reasoned estimate of the analysed risk is the result. Regular and systematic re-assessments are advised due to the dynamic nature of the risk indicators and use of the VERA 2 recommended in combination with other tools rather than as a stand-alone analysis whenever possible. As a complimentary approach, the VERA 2 is able to provide confirmation of an analyst's judgment that is made by other methods such as tradecraft. The VERA 2 supports intelligence analyst judgment and does not replace it. If the multiple approaches provide a consistent outcome, the product is corroborated. If a discrepancy in outcome is noted, the methodologies or tradecraft should be explored to identify the nature and reasons for the divergence.

Validity and reliability issues of the VERA 2

Several important types of validity support the VERA 2. These are addressed independently.

The first of these is "*face validity*". Face validity was granted to the VERA soon after the tool appeared in the open-source literature in 2009 as consultative tool. Face validity refers to the subjective view that a test is going to measure what it claims that it is intending to measure. Levels of face validity can be differentiated, however, depending on the professional expertise and knowledge of the assessors. Inexperienced observers will provide a different level of face validity than highly trained subject matter experts.

In the case of the VERA, face validity was granted by operational experts at the highest analytical level in counterterrorism investigations in a federal and regional law enforcement agencies. The professionals providing the face validity were charged, through work responsibilities, with intelligence and security analysis tasks of violent extremists at the national security level and they found the VERA tool to be of interest to their work. These experts had undergone training in risk and threat assessment and had profound knowledge of the characteristics of violent extremism and terrorism. They judged the VERA protocol and its indicators as comprehensive and relevant to their needs, that is they judged the VERA to have "face validity". Following this judgment, they requested training in the protocol and proceeded with an evaluative application of the VERA in their classified work. The face validity of the VERA was also supported in the high risk correctional setting where a similar judgment of relevance was made by the in-charge senior clinical director of the facility who had the responsibility for undertaking the risk assessments of convicted terrorists incarcerated in this facility. Other tools that had been used in the prison with convicted "terrorist' offenders were not found to include indicators relevant to this population. On the basis of this expert adjudicated face validity, the VERA was implemented in an evaluative protocol within the correctional setting as a "consultative" tool and this was followed by the use of the VERA 2. A formal request for the evaluative use of the VERA protocol was received and granted with subsequent governmental support provided for training and consultations.

While face validity is the most subjective and simplest form of validity, when highly trained subject matter experts provide expert assessment of the relevance of a tool, and allocate both professional time and resources to user training, based on the judged confidence of the tool, the face validity is of a higher standard and can be defined as *"expert adjudicated" face validity*.

To provide more robust investigation, the *content validity* of the VERA 2 was tested using information obtained from subject matter experts in terrorism. Content validity or logical validity refers to the extent to which a measure represents all facets of a given construct. Content validity refers to the set of elements in a measure and to a determination as to whether this set is a comprehensive and representative set. When an instrument contains the set of "necessary and sufficient" indicators for a given construct, in this case violent extremism, then the instrument can be expected logically to measure what it is supposed to measure. Importance ratings on the indicators in the VERA 2 were obtained from professional intelligence analysts working in the area of counterterrorism. These experts were familiar with the characteristics representative of the violent extremists and terrorists. Each of these professionals (n=28) were asked to rate the indicators for their perceived importance in terrorism analysis. The indicators included in the VERA 2 were rated as highly relevant and important, moderately important or not important. There was a high level of agreement by the experts of the importance of the risk indicators included in the VERA 2. Experts were also asked to identify missing indicators that should be included for a more comprehensive set. This task was to determine the completeness of the current set of indicators. Almost all of the intelligence analysts (96.3) indicated agreement with the importance of the set of indicators. This agreement obtained provides strong support for content validity.

Construct validity was also investigated. Construct validity refers to the degree to which a test measures what it claims, or purports, to be measuring and it is deemed to be essential to overall validity. The VERA 2 claims that it will assess the risk of violent extremists and that this risk is different from the risk measured for ordinary violent offenders. The rationale for the development of the

VERA 2 was that ordinary violent criminals are motivated by different elements than violent extremists and that there is a significant difference between these groups that requires distinctive risk indicators. The VERA 2 identifies these elements. To determine construct validity, a group of known violent extremists (convicted terrorists) and a group of known violent offenders were matched as closely as possible on age, sex, ethnic and religious background and compared on the basis the VERA 2 and a risk assessment tools for ordinary criminal violence. The HCR-20, a well known and respected structured professional judgment tool[18]was chosen as it employs the same structured professional judgment method as the VERA 2. A significant difference was found between the groups both on the VERA-2 (p<.01) and the HCR-20 (p<.001). The convicted terrorists were found to have a significantly lower risk level, as was predicted on the HCR-20, and a significantly higher risk level on the VERA 2, relevant measure of violent extremism. The reverse trend was found for ordinary violent criminals who demonstrated a significantly higher level of risk on the HCR-20, a tool for such violence and a lower risk for violence based on ideology. Significant differences (p<.01) were also found between the two groups on a test of psychopathy (PCL: SV).[19] These results support VERA 2 construct validity[20]. Additional testing with larger groups of these two types of offenders is recommended to provide additional robustness for construct validity.

Consumer validity is related to face validity. This validity is based on the experience of the expert user on a posterior basis. This goes beyond the a priori face validity which is not based on an empirical evaluation of the benefits and/or limitations of an approach. A tool is considered to have consumer validity when it is evaluated by expert users and determined to provide practical benefits and utility for the operational work for which it was developed. Consumer validity is an important albeit non-statistical validity because this consumer evaluation determines the sustained implementation of the tool in operational practice. The VERA has been found to have such “consumer validity” with law enforcement analysts, intelligence analysts and correctional psychologists and is expanding in applications. Users have described their willingness to use the VERA 2 and have reported that it is helpful to them and “useful” for their analysis. It has not always been possible for users to obtain information sufficient to permit ratings on all the risk indicators in the VERA 2 but empty cells do not invalidate the approach. The final decision is made on the information available. Further, the empty cells have been found useful for directing the attention of the analysts to seek out the missing information in a consistent manner.

Deductive validity is a form of mathematical induction that links premises with conclusions. It is also called propositional calculus because if premises are true and the rules of deductive logic are followed, then the conclusion must follow and be both true and valid. For example, if a behavior is defined as illegal on the basis of jurisprudence, and a person can be shown to have engaged in the behaviour, then the person has engaged in illegal behaviour. If violent extremism *(x)* is legally defined (by the state) as *(a)* +*(b)* +*(c)* where *(a)*could be the commitment/plan to use violence to further an ideology, and *(b)*could be the actor acts of to support such violence to further an ideological cause; and *(c)*could be that this action is intended to coerce political change by a government and cause fear, then by definition *(x)* = *(a)* + *(b)* + *(c)*. If *(y)* represents a specific person and *(y)*is found to exhibit behaviors consistent with (a) + (b) + (c) then by logical deduction *(y)* = *(x*), that is *(y)* is a violent extremist. This is a result of deductive reasoning and the VERA-2, through the use of risk indicators can apply deductive reasoning to arrive at a deductive validity in the overall risk decision.

Predictive validity is often considered the “holy grail” of risk assessment tools. This is not the case for risk assessment tools for terrorism and violent extremism. This is due to the role of uncertainty in the risk equation and the ambiguity present in some risk indicators. It is due to the dynamic rather than static nature of the indicators that impairs statistical prediction due to potential rapid and unpredictable change. One’s intention to act to support a terrorist action may change rapidly based on an unexpected event.

The structured professional judgment protocol with repeated measures will assist in monitoring such changes an assist in a well-reasoned judgment but not with statistical predictability. The repeated risk level assessments over time will identify micro-risk indicator changes that can contribute to decoding patterns of change and this can also assist in the estimation of future risk using reasoned judgment. The low-base rate of terrorists and the difficulty of access to this population further impairs the ability of researchers to collect the large data samples required for full predictive studies.

One of the fundamental measures of the utility of a risk assessment tool is the extent to which raters can independently assess the same individual(s) and arrive at the same outcome. This level of agreement between assessors/raters is referred to as inter-rater reliability.[21] High levels of inter-rater reliability are an indication that the items that comprise the risk assessment and their coding rules have been clearly articulated. Inter-rater reliability of the VERA 2 protocol was examined in a preliminary study undertaken independently of the author by law enforcement experts. The study included an examination of the agreement in ratings on the VERA 2 by five individuals working in a federal law enforcement bureau. All assessors independently coded four case files using the VERA 2 after gaining familiarity with the rating system and the criterion definitions. Kendall's coefficient of concordance *(W)* was used to assess the agreement among assessors which is a measure of agreement.[22] The *W* for all five raters ranged from a low of 0.55 to a high of 0.78 across the four cases. This is being considered preliminary inter-rater reliability because two raters failed to complete the assessment. A closer examination of the data also revealed a single rater outlier. It was known that this outlier did not have the same training as the other four assessors in risk and threat assessment and when the analysis excluded this less trained and experienced assessor's rating data, the inter-rater reliability improved (*W* ranges from.60 to 0.82). Despite differences in level of agreement among raters across some of the indicator items contained in the assessment among the four cases, experienced raters (n=4) were in 100% agreement on the overall assessment outcome. Slight variations in scoring of individual items did not result in a different risk assessment outcome among all the trained and experienced raters. The high level of agreement in the overall risk decisions in trainees, even when variance occurred in individual risk indicator ratings, has been a pervasive finding. The acceptable inter-rater reliability can be enhanced with the standard level of training (that provided was contracted) and the larger coefficients obtained after the removal of the outlying rater supports the importance of training users with expertise in the field of threat assessment.[23]

Conclusions

Intelligence Services are charged with safeguarding national security, conducting national security investigations and security intelligence collection. The "intelligence" they develop is used to advise governments on both the national security risk posed by individuals within and outside their borders as well as other activities that may threaten the security of the country and its citizens. The accuracy of this intelligence and the validity of the methods used to obtain information are being challenged in the courts of western democratic nations increasingly. This is due to the fact that the "intelligence" produced through the collection, processing and analysis of data produces actionable strategic information that can result in detrimental consequences for citizens. Tradecraft is a weak defence against a charge of analyst bias, unjustifiable intuition, lack of experience, or the use of non-scientific methodology.

The risk posed by violent extremists and the need for their timely identification by intelligence communities exists on every continent. Civil society and governments have the expectation that intelligence communities will provide a competent and accurate analysis of such individual risk with a resulting defensible intelligence product. In the intelligence application, the VERA 2 has been found useful in supporting the professional judgment of analysts and for appropriately challenging analysts when confirmation by multiple analyses does not present the same finding. The assessment of individual risk for violent extremism will always include a component of uncertainty. Although certainty may not be possible in the final intelligence product, adding some redundancy to the system, specifically to the intelligence analysis process, will improve reliability and confidence much as it has done in other scientific fields. Uncertainty in the structured risk assessment does not mean a lack of knowledge.

Feedback on the use of the VERA 2 risk assessment protocol in the intelligence setting has been consistently positive. The VERA 2 has been found to be a useful and practical approach by intelligence analysts and other professionals involved in security and intelligence analysis. Rapid acceptance of the VERA 2 has been facilitated by its use as a complimentary approach rather than as a replacement for other methods used by intelligence communities. The VERA 2 is able to provide support for the analyst's judgment through a useful and structured confirmation of the intelligence product.

References

1. James R. Clapper, Transcript of Remarks to the Senate Select Committee on Intelligence, "Worldwide Threat Assessment", *Capital, Washington*, 29 January 2014, accessed 7 February 2014, http://www.dni.gov/ files/documents/WWTA%20 Opening%20Remarks%20as%20Delivered%20to%20SSCI_29_Jan_2014.pdf

2. *FBI Press Release on Boston Marathon bombers*, 18 October, 2013 accessed 7 February 2014 at http://www.fbi.gov/boston/press-releases/2013/joint-release-from-massachusetts-law-enforcement-agencies

3. Sophia Mosalenko and Clark McCauley, "How Radicalization happens to them and us: Radicalization of Tamerlan and Dzhokhar Tsarnaev", *Psychology Today*, 19 April, 2013 accessed 7 April 2014 at http://www.psychologytoday.com/blog/friction/ 201304/radicalization-tamerlan-and-dzhokhar-tsarnaev

4. D. Elaine Pressman and John Flockton. "Calibrating risk for violent political extremists and terrorists: the VERA 2 structured assessment", *The British Journal of Forensic Practice*, Vol. 14 No. 4, 2012 pp. 237-251.

5. Richard Falkenrath, "Domestic Intelligence and the Boston Bombings", Published Interview: Council on Foreign Relations accessed 8 February 2014 at http://www.cfr.org/counterterrorism/domestic-intelligence-boston-bombings/p30557

6. United States of America Senate Committee on Homeland Security and Governmental Affairs, "A Ticking Time Bomb, Counterterrorism Lessons", 3 February, 2011, accessed 9 February 2014 http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2

7. Siobhan Gorman and Cassell Bryan-Low "Jihadists returning home to Europe from Syria pose new terror threat", *The Wall Street Journal*, 4 December 2013, accessed 7 February 2014 at http://online.wsj.com/news/articles/SB10001424052702303722104579238542737904868

8. *Ibid*.

9. The Canadian Press, "CSIS says some 130 fighters support extremists", 3 February 2014 accessed 7 February, 2014 http://globalnews.ca/news/1126694/csis-says-some-130-canadians-support-foreign-extremists/

10. D. Elaine Pressman and John Flockton, "Violent Extremist Risk Assessment: Issues and Applications of the VERA-2 in a high-security correctional setting" In Andrew Silke *(Ed.) Prisons, terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform*. (Oxon, UK: Routledge,2014)

11. Richards J. Heuer, Jr. *The Psychology of Intelligence*, (Washington, Center for the Study of Intelligence, CIA, 1999), accessed 6 February 2014 at http://www.odci.gov/csi
Also available at http://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art5.html

12. D. Elaine Pressman, *Risk assessment decisions for violent political extremism* Public Safety Canada, (Ottawa, Government of Canada, 2009) Cat. No. PS3-1/2009-2-1E available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2009-02-rdv/2009-02-rdv-eng.pdf

13. D. Elaine Pressman and John Flockton. "Calibrating risk for violent political extremists and terrorists: the VERA 2 structured assessment", *The British Journal of Forensic Practice,* Vol. 14 No. 4, 2012 pp. 237-251.

14. J. M. Post, *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to Al Qaeda*, Palgrave Macmillan: New York, NY, 2007.

15. D. Elaine Pressman, *Risk assessment decisions for violent political extremism*. Public Safety Canada, (Ottawa, Government of Canada, 2009) Cat. No. PS3-1/2009-2-1E available at https://www.publicsafety.gc.ca/cnt/ rsrcs/pblctns/2009-02-rdv/2009-02-rdv-eng.pdf

16. D. Elaine Pressman and John Flockton, "Violent Extremist Risk Assessment: Issues and Applications of the VERA-2 in a high-security correctional setting" in Andrew Silke *(Ed.) Prisons, terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform*. (Oxon, UK: Routledge, 2014).

17. D. Elaine Pressman and John Flockton. "Calibrating risk for violent political extremists and terrorists: the VERA 2 structured assessment", *The British Journal of Forensic Practice*, Vol. 14 No. 4, 2012, pp. 237-251.
18. C. D. Webster, K.S. Douglas, D. Eaves, D. and S. Hart, *HCR-20 Assessing Risk for Violence: Version*, Vancouver: Mental Health Law and Policy Institute, Simon Fraser University, 1997).
19. R. D., Hare, Manual for the Hare Psychopathy Checklist-revised, 2nd ed., (Toronto: Multi-Health Systems, 2003).
20. D. Elaine Pressman, Presentation to a closed meeting for Correctional Services of Norway Staff Academy on violent extremism and radicalization in prison, KRUS, Oslo, March 18, 2013.
21. C. C. Reaves, *Quantitative Research for the Behavioral Sciences*, Mississauga, (ON: Wiley, 1992).
22. P. Legendre, “Species Associations: The Kendall coefficient of Concordance Revisited”, *Journal of Agricultural, Biological and Environmental Statistics*, Vol. 10, No. 2, 2005, pp. 226-245.
23. Unpublished data obtained for VERA 2 inter-rater reliability. Contact the author for additional details.

Methods for Improving Collection and Analysis in Order to Contribute to Non-Proliferation of Weapons of Mass Destruction

Lucian IVAN[*]

Abstract

A more accurate and complete understanding of the full range of WMD threats is, and will remain, among the highest priorities of intelligence services, in order to prevent proliferation.

In this regard, improving abilities to obtain timely and accurate knowledge of adversaries methods and strategies constitute a key element for developing effective nonproliferation policy.

In order to achieve this objective all the efforts must be accorded to improving: intelligence regarding entities interested by WMD, cooperation between intelligence services and law enforcement agencies, as well as intensive cooperation at international level (multilateral agreements in the field of nonproliferation of WMD).

Keywords: non-proliferation, terrorism, dual use technology, weapons of mass destruction

The proliferation of chemical, biological, radiological, and nuclear (CBRN) weapons, commonly named weapons of mass destruction (WMD), as well as their delivery systems (missiles), have the potential to undermine international peace and security and to cause many casualties especially to innocent civilians. Nowadays many countries already possess WMD, or have the capacity to produce them, and an increasing number are in the process of acquiring and developing capabilities to inflict mass casualties and destruction through WMD. While many terrorist groups lack the resources or expertise to employ WMD, there has been a growing interest among certain terrorist groups in acquiring such weapons in order to have a strategic advantage in front of authorities and to launch WMD terrorist acts. The serious issue of proliferation of these weapons has become an urgent matter that international community and many governments are attempting to address.

One solution for non-proliferation is the establishment of mature national strategic trade control systems, which refers to a set

[*] Commissar of police, Ministry of Internal Affairs, Department of Intelligence and Internal Protection, Romania

of government policies, legal norms and practices designed to regulate trade in proliferation-sensitive products for the purposes of preventing the spread of WMD and simultaneously facilitating legitimate trade of strategic goods and technologies. This relatively new concept emerged from the practice of export controls. A few decades ago, when proliferation-sensitive trade was confined to a few key producers, traditional export controls had political underpinnings and suppliers would choose their customers based on strategic alliances. Today, we live in a world in which goods and technology that can be diverted for WMD programs are much more widespread than ever before (an example in this regard could be A.Q. Khan proliferation network). They constitute a significant component of international trade, and the lines between the peaceful and military applications of the same products and technologies are less clearly defined.

Though these systems may seem to be the ideal solution for developed countries, developing countries often question their efficacy and worry about the regimes' effects on their international competitiveness and efficiency. They fear that introducing comprehensive controls on strategic trade will put unnecessary burdens on government agencies and industry, inhibit trade, and divert valuable resources from addressing more pressing development needs.

The reality, however, is far more nuanced and complicated. The WMD threat is not just a concern of Western countries — in a globalized world, even countries without WMD programs or high-tech industries are at risk. What's more, investing resources into proliferation controls does not have to come at the expense of meeting other national objectives and can, in fact, have positive effects in areas such as trade and competitiveness.

Each state must work, to the best of its ability, to prevent WMD proliferation because this is a global issue who can be resolved only through international response and efforts. Governments should have the legal authority and institutional capacity to implement the licensing and control procedures of sensitive trade, as well as the means to enforce any controls they have in place to prevent intentional illegal activity. They should also compile restricted items into a comprehensive national control list who cover all the materials and related technologies who could be used in proliferation activities.

A successful system requires close working relationships between government and industry, and whenever possible, governments should provide incentives to companies to be especially diligent when it comes to sensitive trade. Finally, for a national strategic trade control system to work, close cooperation between countries at the regional and international level is critical.

In these regard we consider necessary to enumerate the most important international mechanisms in place for non-proliferation of WMD:

- **Nuclear & Radiological:** Nuclear Non-proliferation Treaty, Comprehensive Nuclear Test Ban Treaty (CTBT), Nuclear Suppliers Group (NSG), Zangger Committee (ZC);
- **Chemical:** Geneva Protocol (1925), Chemical Weapons Convention (CWC), Australia Group (AG);
- **Biological:** Geneva Protocol (1925), Biological and Toxins Weapons Convention (BTWC), Australia Group (AG);
- **Missile:** Missile Technology Control Regime (MTCR);
- **Other international instruments:** 1540 Committee (implementation of UNSC Resolution no. 1540/2004), Proliferation Security Initiative, European Union Strategy for non-proliferation of WMD etc.[1]

There will never be enough capacity or expertise to fully implement strategic trade controls. But no contribution to the common goal is too small. Working to limit WMD proliferation will make the world safer for all countries and for the next generations.

In order to handling the challenge of proliferation & terrorism with WMD is necessary to have a coalitions of like-minded countries, increasing the importance of Proliferation Security Initiative, increased national efforts and “smart defense” strategies, operations based on intelligence sharing.

States of concern regarding proliferation of WMD

Analyzing the trends of proliferation of WMD worldwide we appreciate that in present countries of concern are represented by Syria (failure state who possess large chemical weapons stockpile), North Korea (totalitarian state concerned in development especially nuclear weapons) and Islamic Republic of Iran (Islamic state who develop a nuclear program of concern for international community).

Syria

Some non-governmental organizations have stated they believe Syria has an active **chemical weapons** program. Syria is not a party to the **Chemical Weapons Convention**, though it denied that it had chemical weapons until admitting it possessed such weapons in 2012. Syria is one of six states that have not signed and eight that have not ratified the **Chemical Weapons Convention**. Syria reportedly manufactures **Sarin, Tabun**, **VX**, and **mustard gas** types of chemical weapons. Independent assessments indicate that Syrian production could be up to a combined total of a few hundred tons of chemical agents per year.[2]

After two years of stalemate, the ongoing Syrian civil war poses a significant challenge for the international community. As many as 100,000 Syrians have been killed, while 2 million refugees have fled the country and another 4 million have been internally displaced. Perhaps most concerning, however, is the eventual fate of the large stockpiles of chemical weapons belonging to the Bashar al Assad regime. While the likely use of chemical weapons against some opposition elements illustrates one horrible scenario, the possibility that the chemical weapons stockpiles fall into the wrong hands in the case of regime collapse is ultimately most worrying to the international community.

The pros and cons of several possible solutions are examined, all within the context of a significant humanitarian crisis and civil war. The desired end state is an extremely critical one, specifically that Syria's chemical weapons and ballistic missiles do not proliferate to a terrorist group. Several radical Sunni Islamist groups, Al-Qaeda affiliates such as the Al Nusra Front, and Lebanese Hezbollah will likely pursue these stockpiles if they perceive that the Assad regime may lose control of any CW sites, or lose power altogether.

General Martin Dempsey, the US military's ranking officer, recently outlined military options for a Syrian intervention. His menu, ranging from remote support to the opposition to the establishment of a no-fly zone, demonstrates the range of Syria's problems. Objectives include toppling the Assad regime, or slowing the rate of death, or at least ensuring some balance to the civil war.

But, his fifth option, one establishing control of Syria's chemical weapons, is arguably most critical to the safety of the rest of the world. Unfortunately, no option (including this one) will be fully successful; something General Dempsey has made clear. And, while securing the chemical weapons may *largely* succeed, it will involve tens of thousands of troops and is hardly politically tenable in the cash-strapped and war-weary West. At this time, this option would lead to a full-scale war with Syria (much like Iraq), and proxy wars with Iran and, albeit less so, Russian Federation. But, immediately after an opposition victory, this may prove viable and could successfully prevent the proliferation of Assad's WMD programs.

A comprehensive "diplomacy-first" approach is ideal. While military planning and intelligence collection should continue, even US military officers have concluded that diplomacy should take and maintain the lead. Some key regional states have advocated a patient approach, even if they must continue to suffer increased instability (e.g. Turkey and Jordan via border incidents). When they have actually occurred, international dialogues have disappointed so far. Russia's largely symbolic identification with the Assad regime is significant, as are Iran's efforts in the country. These "stakeholders" must be acknowledged fully, and engaged seriously. Otherwise, the stalemate from the UNSC on down will set back the "good guys" when the furious scramble for chemical weapons begins. Well before these weapons fall into the wrong hands, non-proliferation must be the focus of negotiations with Russian Federation and regional countries, and even the price for aid to opposition groups. Whether or not diplomacy loses Syria, it cannot lose Syria's chemical weapons.

Based upon our assessment, we consider that the international community continues to work through diplomatic means to encourage an outcome ensuring the continued security of Syria's chemical weapons. Tentative deals with all parties (SNC, Al Nusra Front, neighboring states, Russian Federation, etc.) should be pursued to ensure that an ultimate solution is achieved when the situation rapidly changes in the country. Meanwhile, military options for full or partial seizure or security of chemical weapons sites should be maintained. While a military intervention is not necessary at this time, the international community must be prepared for quick, synchronized, and flexible action – both diplomatic and military – upon the sudden fall of the Bashar al Assad regime.

North Korea

In 1994, United States and North Korea signed the **Agreed Framework** that intent to withdraw from the nuclear **Nonproliferation Treaty (NPT)**, which requires non-nuclear weapon states to forswear the development and acquisition of nuclear weapons**.** Under this agreement, Pyongyang committed to freezing its illicit plutonium weapons program in exchange for aid. Following the collapse of this agreement in 2002, North Korea claimed that it had withdrawn from the NPT in January 2003 and once again began operating its nuclear facilities. The second major diplomatic effort were the Six-Party Talks initiated in August of 2003 which involved China, Japan, North Korea, Russia, South Korea, and the United States. In between periods of stalemate and crisis, those talks arrived at critical breakthroughs in 2005, when North Korea pledged to abandon "all nuclear weapons and existing nuclear programs" and return to the NPT, and in 2007, when the parties agreed on a series of steps to implement that 2005 agreement. Those talks, however, broke down in 2009 following disagreements over verification and an internationally condemned North Korea rocket launch. Pyongyang has since stated that it would never return to the talks and is no longer bound by their agreements. The other five parties state that they remain committed to the talks, and have called for Pyongyang to recommit to its 2005 denuclearization pledge.[3]

According to the Defense agency: North Korea's new leader, Kim Jong-un is more interested in economic reform than in following his father's and grandfather's "military first" policy of bolstering the North's missile and nuclear arsenals, and threatening to use them unless the world came to its door. But the more immediate concern is that Kim Jong-un could follow North Korea's recent playbook and create another provocation akin to the sinking of a South Korean navy ship in 2010 or the recent cyber attack on South Korean banks and news media companies. It took weeks of investigation before South Korea could blame the North for those past provocations.[4]

North Korea's strategy of using its missile and nuclear programs to achieve security, recognition, and aid has been remarkably successful. North Korea receives diplomatic attention from the international community on a scale far greater than its economic and political importance justifies. North Korea has no economic potential, a retrograde political system, and one of the most isolated and repressed populations on Earth. Its political system is maintained only through a combination of international aid and revenue obtained via widespread criminal activities. North Korea has managed to get what it wants from the international community. Using the threat of nuclear weapons and its potential for destabilizing the region, North Korea has drawn the international community into a series of negotiations, from which it gains considerable concessions, including fuel, food, currency, security guarantees, and diplomatic recognition. These strategies have served North Korea well, and set a dangerous precedent for other states which attempts to develop its own nuclear program.

Islamic Republic of Iran

In a 2011 report, the IAEA stated that Iran still refused to cooperate on oustanding issues regarding possible military dimensions of its nuclear program, saying that since 2008 Iran had not engaged the IAEA "in any substantive way on this matter." The report cited Iran's involvement in activities relevant to creating a nuclear explosive, including efforts by military entities to acquire dual-use equipment, to create "undeclared pathways" for nuclear material, to acquire weapons development information through clandestine means, and to test components for a potential nuclear weapon design. The IAEA stated that these activities were part of a "structured program" before 2003, and concluded that they may still be continuing. At the June 2013 meeting of the Board of Governors, Director-General Yukiya Amano said that negotiations between Iran and the IAEA over an approach to resolve these concerns had made no progress after 10 meetings since February 2012.

Iran's stockpile of low enriched uranium (3.5 percent) reached almost 9,000 kilograms by May 2013, of which about 2,500 kilograms has been further enriched to 20 percent. Iran also produced 324 kilograms of 20 percent enriched uranium by this date. However, 142 kilograms were converted into a solid powder to fuel the Tehran Research Reactor, which produces medical isotopes. This reduced Iran's available stockpile of 20 percent enriched uranium to approximately 182 kilograms. Iran continues enrichment of both low enriched uranium and 20 percent enriched uranium.[5]

Further concern was raised when Iran announced that it might build a nuclear-powered submarine, since this would potentially legitimize the country having high-enriched uranium for fuel. It was denounced internationally as simply an excuse for the production of weapons-grade uranium. The potential legitimacy arises from section 14 of the standard Comprehensive Safeguards Agreements signed by non-weapons states. This allows fuel for a “non-proscribed military activity” to evade safeguards.[6]

Technology and WMD terrorism

Technology is a double edged sword in the war of WMD proliferation and terrorism. In many cases, simple and advanced technologies are employed both the state and terrorist actors. This is what is called dual-use technology. GPS, Cellular Phones, Information Technology (IT) and advances in weapons both advanced and crude are exploited by each side. Terrorists use Internet and similar smart phones networks for a variety of reasons, making their work simpler and with a greater reach.

The United States Committee of the Role of Information Technology in Responding to Terrorism wrote “IT also had a major role in counterterrorism – it can prevent, detect and mitigate terrorist acts through the rapid sharing of actionable intelligence”. The use of this technology gives terrorists increased operational capability especially for recruitment, radicalizing, propaganda, fund raising, training, planning, controlling actions and movement of cells and tracking attacks. On the other hand this can be used from the CT side against the terrorists. The fact that terrorists might be using the Internet gives the intelligence agencies a wider opportunity to track them. Without doubt, the modern terrorists need and uses the Internet as much as the AK47 and it is a factor we would ignore at our peril. The rapid leaps in biotechnology, nanotechnology, and neuroscience should increase awareness of their dual-use capabilities as well.

In this regard, the Security institutions must focus on identifying stakeholders, understanding how other countries perceive the threat, and on developing strategies to engage the global scientific community in cooperative methods. Increased cooperation is needed between security agencies and university research centers and private laboratories in order to implement various regulating measures ensuring that they are neither too restrictive nor intrusive to create a problem to the development of technology and science. Regulations and norms should be in place governing the diffusion and sharing of dual-use technology in order to deal with the rapidly emerging technology.

The biggest security issue when we look at technological advancement is the possibility that terrorists might use advanced technology and science as weapons or means to create terror. What increases this fear is the possible magnitude of damage and destruction that can be inflicted to society if advanced science and technology is used as a weapon against them. The wrongful use of this technology can have tragic consequences. If the governments do not invest in prevention, disruption and detection of such threats we believe that the possibility of terrorism and proliferation of WMD being one step ahead of the curve is something that we as a society cannot afford. It is with analysis and assessment of the threats and its consequences in relation to the benefits of technology that we must decide on how much and in what direction governments should allocate their research and development budget.

The intelligence paradigm

In order to prevent proliferation of WMD is needed different type of intelligence[7] such as:

- What information and material need to be protected and denied the proliferation network (where the information and material are located, and the mechanisms for safety and accountability).
- The nature and range of dual-use technology that can be exploited.
- The nature of the global trade in technology and weapons export, and the control regimes supporting their control.
- International financial transfers.
- Local, regional and international terrorism trends.

From the point of view of intelligence gathered we propose the following classification:

- Sensitive-Source Information
  - National intelligence and security agencies
  - Counterterrorism
  - Agents and informers
  - Bilateral information exchange

o International Atomic Energy Agency, Organization for Prohibition of Chemical Weapons, INTERPOL, EUROPOL, United Nations etc.

- Open Source Information
  - o Trade fairs and international trade markets.
  - o Corporate marketing literature.
  - o Scientific and technical media.
  - o Nongovernmental organization community.
  - o Internet.
- Trade-Source Information
  - o Export control requirements and regulatory license applications.
  - o Manufacturers, sellers and brokers.
  - o Import / export documents.
  - o End-user certificates.
  - o Transit routing.
  - o Industry outreach programs.

In order to determine if intelligence is in support of criminal prosecutions or national security operations is needed to have intelligence fusion and databases must allow for regular, routine and nonroutine queries by all relevant agencies.

To gain success in the process of non-proliferation of WMD is necessary to have an integrated policy approach to countering proliferation by adopting and implementing a comprehensive strategy in this regard covering the following items:

- A comprehensive risk assessment.
- Security of potential material and technology targets.
- Protective investigation and intelligence targeting.
- Established mechanisms for information coordination.
- Legal authority to detain and investigate.
- An integrated response plan.

Of course, in order to have an efficient export control of dual-use items and technologies that can be used for production of weapons of mass destruction we must know some “red flags” as follows:

➢ Red Flags for Industry

- o Uneducated or unfamiliar customer.
- o Uninformed buyer.
- o Unusual payment terms.
- o No price negotiation.
- o Vague or non-existent end-user information.

- Late change in deal terms and/or source of payment.
- Hand-carry of data or equipment.
- Product does not match license.
- Merchandise returns or repair request from wrong customer location.

➢ Red Flags for Academia

- Multiple requests for identical product or research.
- Uneducated, unfamiliar and/or uninformed end user.
- Suspect end-user located in a transhipment location.
- Offer of overpayment.
- Threatening the withdrawal of contact if export license is required.
- Attempts to insert an academic export control exemption to a contract where none apply.

Emerging threats and trends in WMD proliferation and terrorism

As we consider the future link between technology and WMD terrorism, it is essential to consider the possible contextual situation in which the emergence of new weapons might impact on society.

Admittedly, attempts to predict the future are fraught with difficulty. There is rarely, if ever, a standardized perspective on what circumstances will exist over the short to medium term and indeed no certainty on what length of time is germane to such a study. Identifying potential weapon types in alternative future scenarios is by definition imprecise and therefore must be caveated with the risk that some or all, alternative futures, might never come to fruition.

Nevertheless, the points of view below offer one such possible future, based on the extrapolation of trends from a number of horizon-scanning studies, informed research and analysis and known social and technological developments.

From the point of the ***future global landscape*** we have identified the following perspectives which could affect trends in WMD proliferation and terrorism:

➢ Vast economic and social disparities in a globalised community.

➢ Resistance of fragile and failed states to external pacification and development.

➢ The rise of new ‘city states’.

➢ Emergence of global elites divorced from traditional political concerns.

➢ The fragmentation of state monopoly on violence and rise of complex and sophisticated alternative security structures.

➢ The emergence of 'values warfare' around single issues such as religion, environment or energy.

➢ The development of global bio-surveillance.

The ***future technological landscape*** will be influenced by the following factors and trends:

➢ Significant disparities in access to cutting-edge technologies.

➢ IT and Communications key drivers of modernity.

➢ Public health.

➢ Knowledge acquisition closely monitored and controlled.

➢ Disparities in global means of production.

➢ Travel and commerce e-based – pilotless and remote operations.

➢ Disenfranchised communities within larger virtual world communities.

➢ Evolution of proto-cyborg humanity.

A new concept arises from the reality of XXI century, respectively ***neo-terrorism*** characterized by the following concepts and trends who pose a constant risk to public order and security stability:

➢ Terrorism a life-style choice – more self-selection and less grooming.

➢ The rise of 'mercenary terrorism' organized groups – possible links to crime.

➢ Greater decentralization of leadership and operational control.

➢ Complexity of ethical and moral base – shifting allegiances, no boundaries and violence linked to pathologies of individuals.

➢ Willingness to embrace 'exotic weaponry'.

Taking into account the recent development in the field of security at international and national level we could forecast the ***future trends*** in this domain, respectively:

➢ The demise of state investment in security – replaced by private, corporate and communal security.

➢ Unrecognizable developments in technical surveillance to support pre-emption.

- The development of hybrid security officers – blending national security/law enforcement/public health.
- Enhanced lethal and non-lethal arsenals.
- Significant changes in traditional legal forms.
- Greater use of correctional facilities linked to medical practice.

WMD terrorism represents more and more likely ***the weapons of choice of terrorist organizations*** and could be influenced by the current developments in the following domains:

- Significant developments in IEDs.
- Cyber.
- Remote and pilotless platforms – drones, ships, cars, aircraft.
- Nanotechnology.
- Wave, Light and pulse weaponry – Lasers, EMP, Tidal.
- Robotics.
- Bio-terrorism.
- 3D Laser Printing.

Acquisition, sourcing and fabrication of Weapons of Mass Destruction could be influenced by the following factors:

- Easy accessibility to dual-use technologies.
- Greed, diluted ethics and morals and technical curiosity will empower many individuals.
- Little or no need to transport materials and components.
- Testing concepts and plans on virtual platforms.
- Enhanced Insider Threat.
- New forms of e-bay style proliferation markets.

In this regarding we consider that ***the main challenges for government's entities*** represent:

- Regulations and Legal norms.
- Ethics.
- Surveillance.
- Controlling key non-state actor stakeholders.
- International cooperation.
- Suppressing motivations.

Although much of the above must remain speculative, it nevertheless offers a possible platform against which to assess the impact of the technology and weaponry which might be developed and deployed by a non-state actor acting with malicious intent.

References

[1] Lucian Ivan, Anca-Gabriela Petrescu, Izabel-Daniela Ivan, Iulia Companis, *Elemente de management al prevenirii si combaterii utilizarii armelor de distrugere in masa – vol. 1* (Ploiesti: Editura Grafoanaytis), p. 10-11.

[2] *Syria and weapons of mass destruction*, accessed 22 August 2013 on http://en.wikipedia.org/wiki/Syria_and_weapons_of_mass_destruction

[3] http://www.armscontrol.org/factsheets/dprkchron, accessed 22 August 2013

[4] David E. Sanger and Choe Sang-Hun, *Intelligence on North Korea, and Its New Leader, Remains Elusive,* accessed 22 August 2013 at http://www.nytimes.com/2013/05/07/world/asia/intelligence-on-north-korea-still-out-of-reach.html?

[5] *Arms Control and Proliferation Profile: Iran*, accessed 22 August 2013 at http://www.armscontrol.org/factsheets/iranprofile

[6] *Nuclear Proliferation Case Studies*, accessed 22 August 2013 at http://www.world-nuclear.org/info/Safety-and-Security/Non-Proliferation/Appendices/Nuclear-Proliferation-Case-Studies/#.UhXZsZKyDZY

[7] Richard Hoskins, 13-8 Seminar on Combating WMD and Terrorism, 30 July – 9 August 2013, Marshall Centre for Security Studies, Garmish-Partenkirchen, Germany, *WMD Proliferation Pathways: An overview*.

Prospects of Social Media Intelligence Exploitation on the Social Networks

Silviu NATE[*]
Sergiu Tudor MEDAR[*]

Abstract

Social media represents a definable concept but difficult to decipher because of it extremely ample dynamics. Twenty years ago, it was difficult to anticipate the extent that technological dynamics would force a new social paradigm. Online platforms, software and hardware market evolves almost exponentially. Trying to capture the effects of social media and understand the behavior and motivations substrate is both a scientific challenge and a cultural one. Thus, we observe, in developed countries, a trend to digitize and become technically completely mobile. Technology accessibility and the constant stream of mentions on online social networks and blogs provide an opportunity for companies to monitor their products, services, brands and consumers in social media. Equally, scanning, analysis and interpretation of online information to determine the motivations of users bring added advanced knowledge. Consequently, there is no intelligence without interaction, and Social Media Intelligence (SOCMINT) has significantly changed the way brands and marketers leverage social media for business.

Keywords: Social networks, business, analysis, intelligence, cyber space

Conceptual context

Technology accessibility and era of information overload brings the need of learning how to comprehend and extract the information which is useful for the majority of the companies or governments. Constant stream of mentions on online social networks and blogs provide an opportunity for companies to monitor their products, services, brands and consumers in social media. There is no supreme prototype on the market for effective monitoring or a perfect tool that is using the most elaborate algorithms. But there is a constant need for understanding the human factor or the real human selection behavior for setting up human motivations and values.

[*] PhD. Assistant professor, “Lucian Blaga” University of Sibiu, Romania
[*] PhD. Professor, “Lucian Blaga” University of Sibiu, Romania

Diagnosing social media interactions and shared content in relation to business targets is significant. Whether we filter information through a market monitoring tool or via different platforms, regular scanning allows a company to be responsive and to adjust business processes. From the state level point of views, the spectrum of threats forces to adapt from traditional spy tradecraft and to applying it to the cyber world. The complex world will develop more sophisticated tools to assault or to protect the cyber environment.

Social media is the world's largest focus group with millions of participants sharing their unprejudiced opinions daily and social media is quickly becoming an affordable alternative for deep research. With this giant data set, participants now have the power to extract and further comprehend consumer opinion and disseminate information by gender, age segmentation and location.

Social Media Intelligence (SOCMINT) is a concept used by a large number of private companies, but is insufficiently clarified. It is rather a chaotic approach, but under the pretext of search for quality, the ultimate goal is quantity. In this case, the major risk is that consumers will be minimized stage of fixed asset. The increased level of dependence gets stronger pillars that are not sustainable and risk emphasizing a gap on the real motivations and reactions of suppliers and consumers, thus undermining quality research. As a consequence we arrive at ethical issues that require a distinction between the manipulation of the customers and the search for quality in order to develop and deliver better products or services. The quality of communication is developed on the identification of a common value system that undoubtedly will lead to understanding the motivations of the parties involved and to eliminate disparities.

In this sense social media is not good or bad, but SOCMINT comes as a scientific alternative/tool, and uses the selection, filtering and interpretation of a large mass of information, making a distinction between generalization and customization, between qualitative and quantitative approaches, between values and motivations, and between ethical and non-ethical perspectives.

Virtual communities are the expression of participatory mechanisms on various segments, and by extension, the SOCMINT, would provide a certain level of consumer's informal representative for the company's decision making process.

Methods proposed for scientific SOCMINT output

Data mining is used for automatic and/or semi-automatic analysis of large quantities of data to extract previously unknown interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection) and dependencies (association rule mining). These patterns can then be seen as a kind of summary of the input data, and may be used in further analysis or, for example, in machine learning and predictive analytics.

Cluster analysis formulated as a multi-objective optimization problem that involves trial and failure. It is able to modify preprocessing and parameters until the result achieves the desired properties. It is also possible to use a number of terms with similar meanings, including automatic classification, and numerical taxonomy.

Quantitative marketing research based on interactive processes in which both the buyer and seller reach a satisfying agreement on the “four Ps” of marketing: Product, Price, Place (location) and Promotion. Using specific steps for: conceptualization and operationalization, hypothesis specification, establishing scale indicators, data collection, statistical analysis, interpretation/ integration of findings.

Content analysis or textual analysis capable to include large amounts of textual information and systematically identify its properties, e.g. the frequencies of most used keywords by locating the more important structures of its communication content. It is an significant tool in the measurement of success in social media environment and the assessment of media profiles.

Regression analysis and linear regression is used to fit a predictive model to an observed data set and be utilized for multivariate and independent univariate tests. Reducing percentage errors is useful in the field of forecasting or time series analysis.

Case study or case report as an intensive analysis for other similar systems that are studied with mentioned methods, using approaches for theory-testing, theory-building or illustrative, having a retrospective and anticipative value.

Longitudinal study for correlational research study that involves repeated observations of the same variables over the same segment of consumers. It allows also distinguishing short from long-term phenomena and has relative power to detect causal relationships between end-user and provider but also suggests decision-making hypothesis and benchmark management process.

Multi Attribute Decision Making (MCDM) and Multiple-Criteria Decision Analysis (MCDA) - customer satisfaction and the cost of providing service are two conflicting criteria that would be useful to consider. Structuring complex problems and considering multiple criteria explicitly leads to more informed and better decisions by separating strategic knowledge from the consequences of such decisions that are made based on only intuition.

Intelligence analyses – develop analytic synergy for strategic, operational, or tactical solutions in order to achieve competitive advantage.

We consider that the aim of integrating the above scientific methods is to explore and to generate trans-disciplinary alternatives and connections for Social Media Intelligence from conceptual/ theoretical perspective to practical implementation analyses. In that order, researches will produce a valuable tool for strategic decision making and will benchmark processes based on advanced knowledge of the authentic demand and market's dynamics.

Another major challenge is to understand the behavior of consumerist environment offered by transparency and access to diverse open sources of social media. The analytic tool is aimed to provide intelligent consumer's feedback, and become a functional resource for company's quality out-puts. Technological paradigm raises both of cultural and ethical issues. Using scientific methods we are aimed to avoid undesired surprise and discordances for implicated actors.

The whole vision for intelligence tradecraft is part of a comprehensive thinking system. As a subcomponent, the analytical scanning model should be able to fit into mathematical and IT interpretation schemes. Methods proposed specify its interface with the entire comprehensive thinking system. It will define and provide practical models or similarities for future implementation development.

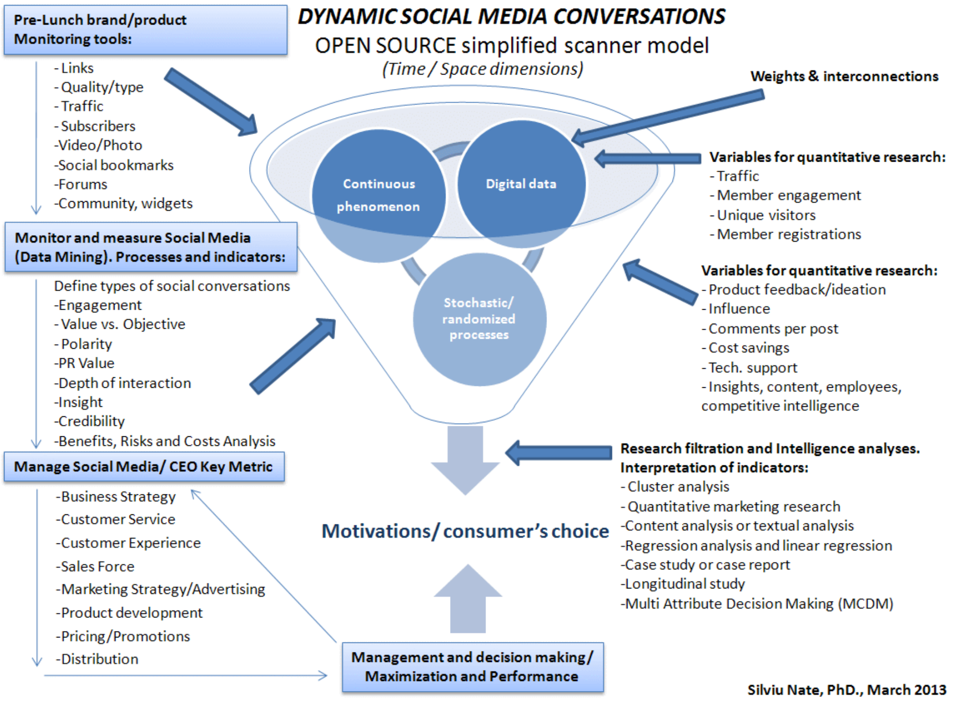

DYNAMIC SOCIAL MEDIA CONVERSATIONS
OPEN SOURCE simplified scanner model
(Time / Space dimensions)
Pre-Lunch brand/product Monitoring tools:
- Links
- Quality/type
- Traffic
- Subscribers
-Video/Photo
-Social bookmarks
-Forums
-Community, widgets
Monitor and measure Social Media (Data Mining). Processes and indicators:
Define types of social conversations
-Engagement
- Value vs. Objective
- Polarity
-PR Value
-Depth of interaction
-Insight
-Credibility
-Benefits, Risks and Costs Analysis
Manage Social Media/ CEO Key Metric
-Business Strategy
-Customer Service
-Customer Experience
-Sales Force
-Marketing Strategy/Advertising
-Product development
-Pricing/Promotions
-Distribution
Continuous phenomenon
Digital data
Stochastic/ randomized processes
Weights & interconnections
Variables for quantitative research:
- Traffic
- Member engagement
- Unique visitors
- Member registrations
Variables for quantitative research:
- Product feedback/ideation
- Influence
- Comments per post
- Cost savings
- Tech. support
- Insights, content, employees, competitive intelligence
Research filtration and Intelligence analyses. Interpretation of indicators:
- Cluster analysis
- Quantitative marketing research
-Content analysis or textual analysis
-Regression analysis and linear regression
-Case study or case report
-Longitudinal study
-Multi Attribute Decision Making (MCDM)
Motivations/ consumer's choice
Management and decision making/ Maximization and Performance
Silviu Nate, PhD., March 2013

Fig. 1 – *Corporate needs and interests vs. scientific approach (Source: Nate, S.© , Common and distinct SOCMINT)*

As a short example:

General pattern of thinking that underlies the scheme refers to the registration of consumer perception about launched products or new brands.

Thus, from a total mass of information will determine specific segments *(S)* for scanning information available on social networks or other online (open sources) communication interfaces.

Variables are preset on the surface of a scan segment, having also the possibility to identify new variables related to consumer preferences and behaviors through data mining techniques.

X, Y, Z become variable of S.

The process model is developed for analyzing large amounts of data and extracts relevant information using mathematical and statistical methods.

Data Segment S(x,y,z) = F(x,y,z) is consumer preference/ perception or motivation/choice $S^n[1, \dots , q, \dots , r)$;

If they, in turn, can vary as functions of time, we have:

$S = F \{x(t), y(t), z(t)\}$

Thus we have fields of criteria (type) which may change dynamism.

If time is a phenomenon of stochastic random variable *(v),* then:

$S = F \{x(v), y(v), z(v)\}$.

And if stochastic variable is dependent on external factors *(e)* or larger phenomenon like changes in the market or competitors strategic moves, we have:

$S = F \{x(v(e)), y(v(e)), z(v(e))\}$

If repeatable phenomena are dynamic, they are:

a) be described by a single frequency *ωo;*

b) if there are more complex, are described by a function description (DF) as a series or a sum of several functions with weights dependent and down, depending on the number of frequencies in the range *(ωo,1,2,...,7 maximum)* multiple frequencies seem, odd or both of the main frequency *ωo.*

Using this logic we can mainstream social sciences in those instruments of analysis and reconstruction wavelets used in forecasting and decision random phenomena.

Social media intelligence gives actionable insights into business and detailed segmented information about consumers. A social business becomes customer-centric and social media enables more effective engagement, learning, and adaptation.

Regression analysis will partially determine objectivity instead of ambiguity and articulates purchasing decision. Social media research can quantify and qualify which step in the path to purchase continuum is stopping consumers dead in their tracks.

The example outlines the rational view and the subsystem's approach specificity able to simulate real and scenario cases.

Innovation, brand health, marketing optimization, revenue generation, operational efficiency and customer experience represent direct benefits of SOCMINT.

Transdisciplinary research

The big challenge is to understand how to develop and implement coherent SOCMINT, both practical and conceptual. Therefore it is very necessary to have a scientific understanding, sociological tools to work with and finally avoid speculative approaches.

The need to improve SOCMINT will develop the research centered on identifying consumer values in order to determine their motivational choices. Consequently, the sociological method shall *translate values into behaviors* and the potential mathematical transpositions will capture the incidence and the congruence of these values. This secondary step contributes with tangible data to interpret and to correlate processes on consumer behavior and decision-making.

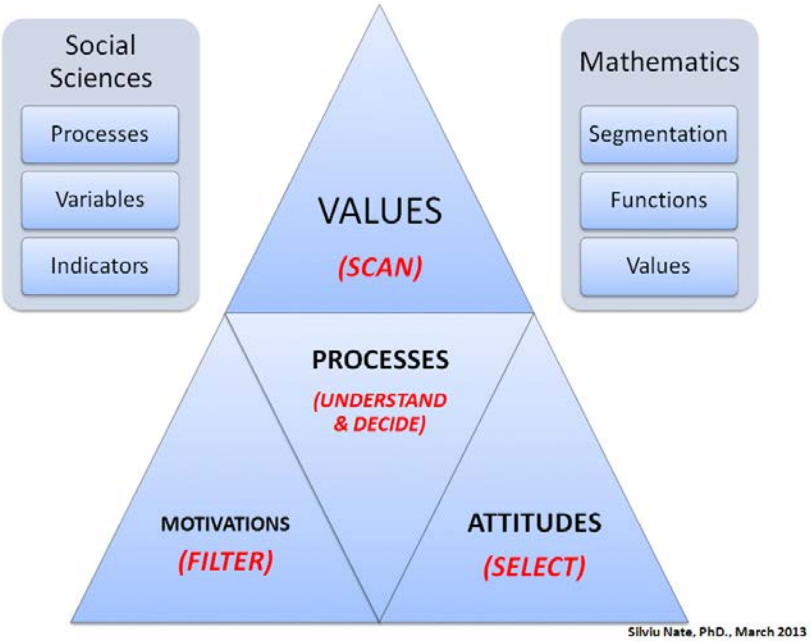


Figure 2 – Non-Chaotic Systems – Diagnostic and Prediction
(Source: Nate, S©. Tangible and intangible values)

Because no social analysis produces results with absolute truth, where necessary, intuition will be supported by advanced concrete knowledge and stochastic systems.

Social and behavioral analysis supports prediction and consistency, having the opportunity to correct decisions on the go to new situations.

Social Media Intelligence tools should try to overpass the real and present danger in trying to quantify things that can't necessarily be quantified. Mathematical arguments are considered precise because they are grounded in formal logic, and when the softer sciences try to make use of a mathematical style of argumentation, decision makers often do so with not the best of intentions. An integrated analytic system will hesitate to misappropriate the certainty of mathematics by camouflaging premises as mathematical statements.

A major challenge of SOCMINT is to grasp the extent to which new technological paradigm influences social dynamics. Such understanding shapes strategic vision for both businesses and consumers. A strategic vision brings academia closer to corporate, thus becoming a generator of innovation in step with market trends, but also to support an objective attitude sustained of values.

Research mechanism's findings will be able to provide recommendations for decision-making and social behavior.

Scanning and interpreting social behaviors that are supported by participatory online platforms will identify unitary and dissipated visions; will provide dialogue, reactions and constructive feedback. Finally, from the position of the third actor, the research results can expose the values that support both sides (provider vs. consumer), and thus determine the real motivations on the market and the so-called social dynamics.

Mathematical and social approaches are interrelated, such as: system vs. subsystem, functions vs. variables and processes, mathematical values vs. social indicators. Social Media Intelligence concepts and tools will be defined and correlated, and then subjected to algorithmic process.

Many of the consumer's choices are subjectively considered by companies in case of failure. On a scheme of advanced Social Media Intelligence analytic tool is possible to categorize rational or irrational end-user's choices and to identify the assigned utility for both sides. A major task is to establish the interest incidence point of goods provider and consumers. Assigned utility would be a central key for generating algorithm and a foundation for shaping future optimal SOCMINT strategy. Therefore, SOCMINT would sustain implementation for Multi Attribute Decision Making (MCDM) and Multiple-Criteria Decision Analysis (MCDA).

SOCMINT challenges

According to Wikipedia list of social networking websites, there are more than 250.000 sites that call themselves social networks. In order to get maximum results from company public relations efforts, it needs to spend time identifying the media channels that its audience trusts.

Social media networks are real platforms where:

- people could advocate companies or governments;
- people are able to collaborate on participatory basis;
- people produce content about products or services;
- people engage behind a company.

Without an ethical approach for SOCMINT to generate a fair relationship based on respect for consumer through participation and transparency, this tool would easier become a vector for manipulation. Tangible values for accountability would provide higher efficiency for companies' internal and external environment. The final outcome and prediction are not measurable only by revenue of investment; the company's inside management transformation and cultural adaptation produce add value for positioning on market. The scientific approach gathers scientific knowledge and practical result for a competitive intelligence approach. But the main question remains: what is the real value of social media conversation?

To determine the most appropriate step to start a SOCMINT clarification, a new question arises: *What's happening more quickly: social media is becoming more traditional or traditional media is becoming more social?* What influences informational environment, the complex technology or diversity of human reactions? As we stated at the beginning, we believe that a new technological paradigm will generate a new societal paradigm. It is important to explain that "open" does not equal "free". Budgets are limited, and so "you have to make a choice as to which sources need to be exploited in order to comprehensively understand and answer a given intelligence requirement. This very selection calls for considerable knowledge of the media landscape, its actors, capabilities and interests, and it calls for a collector's integrity to resist the temptation of ignoring sources that are not easily (or cheaply) available"[1].

SOCMINT assessment is also valuable to understand public opinion regarding political issues. RAND Corporation presented in 2009 an analysis of Iranian public opinion and mood as expressed over Twitter in the nine months following the election. The research represents an initial case study of a novel methodology developed to analyze politically oriented social media content[2]. The program of research into social media would be able to explore not only those media that are primarily text-based (e.g., Twitter), but also the content associated with these video sites (e.g., YouTube). A first step in analyzing video-based social media would be to identify the number of users who reference a YouTube video and possibly the actual video itself (if the URL is embedded in the text). Other analyses focused on YouTube could examine transcripts of the videos, comments made in response to the videos, or the referring sources from which they were linked.

Conclusions

By understanding the line between what is “free” and what means “open” source, intelligence structures prefer to maintain anonymity about their identity from online users or to protect from other competitors and do not lose their own informational heritage. Various numbers of private companies are hiding their identity when actually penetrating sites or other online databases. On the other hand, is expected an increasing number of private companies that will use software to protect their business heritage and strategy by sheltering open source information to not become an open source intelligence for others.

Social media are ideal tools for monitoring, listening and responding to the media and the public. No online platform today is built without offering metrics. Some common examples include:

- Google alerts
- Facebook Insights
- YouTube Insights
- Twitter analytics
- Bit.ly analytics

Dynamic environment requests dynamic approach and understanding. There are no absolute answers, but we find potentials for closer reality to human behavior understanding. The most visible attribute is that social media keeps changing, people get digital by using new platforms and new multimedia facilities day by day. As a result, Social Media Intelligence's ultimate target is to understand motivations and choices of people, through values.

An extended tool for SOCMINT output on the market is "war room" but it should be efficiently mastered. If the "war room" will not adapt the strategy to opinions and consumer's motivations, it would simply become an undesired propaganda machine that would not lead to internal and external quality improvement but it may possibly intoxicate and clear away public empathy.

References

[1] Florian Schaurer, *"Open' Does Not Equal 'Free"*, accessed 24 March 2013, at http://osintblog.org/?p=1617

[2] RAND Corporation, *Using Social Media to Gauge Iranian Public Opinion and Mood After the 2009 Election*, accessed 24 March 2013, at http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1161.pdf

Identifying Risks and Threats to Romania's National Security. A Sociological Approach

Cristian BARNA[*]
Valentin NICULA[*]

Abstract

Numerous approaches on the concept of security and the rise of numerous schools of thought within the security policies direct us towards a complex interpretation of security. The decisions, the policies and the strategies are greatly influenced by the paradigm in which we stand. The effectiveness of the interpretative horizon depends largely on innovation, complexity of analysis and the interdisciplinarity of security studies.

A mature approach to the issue of national security, based on advisory relationships and permanent feedback elements from the academic level, private experts and civil society to the top of the political pyramid, will eliminate some of the frustrations and false perceptions of the Romanian society on security institutions.

Keywords: risks, threats, outranking method, national security, prioritization

Introduction

The international security environment is rapidly changing and the proliferation of new risks increases the insecurity issues of the global environment. For this reason, in the upcoming seven years, the world order will look significantly different, as the new dynamic of international relations promotes the Euro-Atlantic community's efforts to build a new international balance.

By 2020, the international system will be a global multi-polar one with gaps in national power continuing to narrow between developed and developing countries. Concurrent with the shift in power among nation-states, the relative power of various non-state actors is increasing.

Nowadays, the security environment is mainly characterized by the following major trends: the acceleration of globalization and regional integration, along with the persistence of actions that aim

[*] "Mihai Viteazul" National Intelligence Academy, Romania

[*] "Mihai Viteazul" National Intelligence Academy, National Institute for Intelligence Studies, Romania

state fragmentation; reasonable convergence of the efforts made to structure a new security architecture, stable and predictable, accompanied by heightened anarchic tendencies in some regions, renewed efforts of the states to preserve their influence in the international relations dynamic, along with multiple forms of intervention and increasing the share of non-state actors involvement in the evolution of these relations.

Although, after the terrorist attacks of September 11, 2001, the decision-makers and analysts claim in unison that "the world will never be as it was" few were those who really "saw" how the world will change the next decade of the "exceptionalism" of the "global war on terror", the geopolitical cutout of the 3rd millennium debut!

Now, the same decision-makers and analysts are wondering how the world has changed in these years and what is the next big geopolitical cut that will make the world to no longer be the same as it was in the near future: be it information explosion versus "big brother", famine, natural disasters or nuclear disaster?

All these and many more are variables of some prospective scenarios generating security strategies that mark our present and will determine our future! A good example of this is how political developments in Ukraine, in 2014, which few analysts would have anticipated, have affected the regional balance of power (if not global!). Also, these regional developments overshadowed all the great geopolitical topics in 2013: the Iranian nuclear file; the Syrian civil conflict or the tensions between Sunnis and Shias in Lebanon. The Snowden case; ISAF troop withdrawal from Afghanistan or the rebranding of Al Qaeda are no longer hot questions on the media agenda regarding the analysis of international relations!

However, these geopolitical realities of the third millennium should not be ignored! They are on the "to do list" of strategy-makers in a world where they are constrained in conducting their analysis on the need to prioritize the efficiency of resource use in the decision-making process!

Therefore, prioritizing risks and security threats is not a goal but an intrinsic condition in developing security strategies at international, regional and national level.

Romania either should not have a different approach in this regard! Prioritize risks and threats to the national security of Romania give decision-makers the possibility of conducting a clear and concise analysis of security strategies, using the mapping and quantification process. Also, such an approach can provide an analytical substrate to decision-makers of law enforcement, defense and national security structures to connect in a more flexible and efficient way to the tasks set by policy makers and to ensure the adaptability and the interoperability of several categories of forces involved in the prevention and counter of these risks and threats.

Outranking method

Prioritizing methods establish the relative value of choices or alternatives answering the question: “what's the most important?” In this respect, we can prioritize results in a ranking of the choices to show what should be done first, what requires the greatest attention and what needs the most resources. Methods differ depending on whether the priorities are based on objectives or criteria.[1]

Formal multi-criteria analysis techniques usually provide an explicit relative weighting system for the different criteria. The criteria represent the “judging standards” that should be complete, operational, decomposable, non-redundant and minimal in size. The main role of the techniques is to deal with difficulties that human decision-makers have been faced by in handling large amounts of complex information in a consistent way. A key feature of this method is its emphasis on the judgment of the decision-making team in establishing objectives and criteria estimating relative importance weights and in judging the contribution of each option (alternative).[2]

In order to support the decision-maker who must solve multi-criteria problems, three kinds of methods were essentially considered: aggregation methods using utility functions, interactive methods and outranking methods. The outranking methods consist of a compromise between the too poor dominance relations and the excessive ones generated by utility functions. Every outranking method includes two phases: the construction of an outranking relation, the exploitation of this relation in order to assist the decision-maker. The valued outranking graph, when obtained, offers the decision-maker much valuable information.[3]

It is thus essential for decision makers to be able to see to what extent changes of the weights of the criteria will impact the rankings provided by a multi-criteria method.[4]

On the basis of this the decision-makers can set about deriving the relative importance of the criteria and then assessing alternatives against each criterion.[5]

The preference ranking organization method for enrichment of evaluations and its descriptive complement geometrical analysis for interactive aid are better known as the Promethee & Gaia methods. It is used around the world in a wide variety of decision scenarios, in fields such as business, governmental institutions and education, providing the decision maker with both complete and partial rankings of the actions. The applications of Promethee & Gaia to complex multi-criteria decision scenarios have produced extensive results in problems involving planning, resource allocation, priority setting and selection among alternatives.

Prioritize risks and threats to the national security of Romania in 2013 and 2020

For this reasons and given the geopolitical context sketched in the previous chapters, we considered useful and necessary to conduct a research to provide a picture of how students engaged in university master programs in national security and intelligence analysis (future decision factors, analysts and opinion leaders in the field) are prioritizing risks and threats to the national security of Romania.

In the first phase of the research, we conducted a content analysis on two of the most important strategic documents on national security and defense in Romania: "Romania's National Security Strategy. European Romania, Euro-Atlantic Romania: for a better life in a democratic, secure and prosperous country"[6] (2007) and "Romania's National Defense Strategy. For a Romania that ensures the security and prosperity of future generations"(2010) [7]

Following the content analysis performed, there were identified the following risks and threats to the national security of Romania and several vulnerabilities and failures that can amplify them:

- The danger of a classical war and a conventional military aggression.

- Risks and threats to the security of national borders.

- International terrorism: the challenge of massive loss of life and material destruction on a large scale.

- Terrorist groups access to weapons of mass destruction.

- Financing of terrorist groups.

- Proliferation of weapons of mass destruction: the possibility of using such an arsenal for military operations, and the emergence of non-state entities able to acquire some capabilities of producing weapons of mass destruction.

- Ballistic missile development programs.

- Regional conflicts: the strategic area that is located Romania is still rich in local conflicts, ethnic or religious, along with other tensions, separatist tendencies, territorial disputes and situations of instability.

- Proliferation of radical, extremist or irredentist manifestations may affect the rights and freedoms of citizens, social cohesion and inter-ethnic relations.

- Transnational Organised Crime: Romania is a source, transit and destination area of criminal activities consisting of: illegal trafficking in weapons, ammunition and explosives; narcotics trafficking; illegal migration and human trafficking; trafficking in counterfeit goods; money laundering activities; other aspects of economic and financial crime.

- Informational aggressions generated mainly from the international environment, but also by some internal entities.

- Espionage and other hostile actions of the intelligence services and other activities of non-state actors oriented on influencing the decision process, the media or the public.

- Inefficient management of public affairs: failing to exercise responsible and efficient use of power, in accordance with the principles of democracy and human rights requirements, diminishing the ability of law enforcement by some state institutions; low administrative capacity at central and local level; excessive politicization of institutions, both locally and nationally; corruption, with implications for the functioning of state institutions and negative effects on the lives of citizens; lack of a coherent mechanism for forecasting, forecasting, scheduling, planning, execution and control to support budget management system based on multi-annual results; budgetary imbalances caused by bad political decisions.

- Ineffective government (budgetary imbalances caused by wrong political decisions): the effect of the democratic deficit and institutional corruption undermines citizens' trust in public institutions.

- Serious Geophysical phenomena, climate change or related to that or reflecting from environment degradation, including as a result of human dangerous or reckless activities: natural disasters or other events or geo-severe weathering (earthquakes, floods, global warming and other sudden and radical living conditions); the trend of exhaustion of vital resources; industrial or environmental disasters, disruption of economic and social life and serious environmental pollution in the national territory and adjacent regions; increased possibility of pandemics.

Risks and threats to national security can be enhanced by some vulnerabilities and shortcomings: dependence on resources hard to access; negative persisting demographic trends (negative demographic trends and population aging), massive migration (family cohesion degradation as a result of the migration phenomenon, with very negative consequences on children and youth); high level of social insecurity, chronic persistence of poverty and increased social differences; low proportion of fragmentation and the role of the middle class still insufficient in organizing economic and social life; fragility of citizenship and solidarity; poor infrastructure and insufficient protected (weaknesses in critical infrastructure protection and operation); precarious and low efficiency of the health insurance system (lowering the quality of public health services); organizational flaws, lack of resources and difficulties of adapting the education system to the demands of society (the poor quality of the education system by degradation of education, with direct effects on the evolution of Romanian society through its de-professionalization); inadequate organization and management resources scarcity crisis; insufficient involvement of civil society in the debate and solving process of the security issues.

After identifying these risks, threats, vulnerabilities and disruptions to the national security of Romania, as they are mentioned in the policy documents analyzed, in the next phase of our research we have applied the technique of content analysis to identify how they are found listed, in particular, in the analysis of experts in security studies, defense and intelligence in Romania, as well as how it is reflected on the public agenda and the Romanian media. Following this analysis a list of 99 items was built and the 100th was left to respondents to be detected if they could identify other risks, threats, vulnerabilities or malfunctions to the national security of Romania.

Subsequently, after listing the indicators it was developed a questionnaire filled by respondents who were asked to compile a ranking of indicators in descending order of danger they think it would generate to the national security of Romania in 2013.

After the application of questionnaires, respondents have identified the following risks and threats to national security, they have subsumed to indicator I.100: settling of accounts between organized crime groups as terrorist attacks, disintegration of production sectors by bankrupt state companies slated for privatization, mismanagement in state firms, running out of domestic capital in the country by offshore companies, excessive privatization and lack of state control over important elements of the Romanian economy, weak health and social insurance system to respond to an increasingly aging population and face underfunding relative to the rate of social contributions collection in continuing reduction, purchasing most of the products that run on software from foreign producers (e.g. China), dependence on commercial and military satellites of other countries, there is a gap in terms of research (which will create a dependence on technologically advanced countries in the field of IT, nano-systems and microsystems, photonics, robotics, health) threats caused by the emergence of very serious virus that put public health at risk, intentional attacks on people with special viruses created in the laboratory, the proliferation of violence and lack of strategies / laws to combat this phenomenon, regionalization / autonomy too high in regions where are the majority ethnic groups, multilateral development of China, the national currency depreciation, low rate of absorption of EU funds, the involvement of international institutions (like the IMF) in Romania budget management, demographic aging could generate import labor and thus increase the number of foreigners (which ultimately could lead to social unrest and xenophobia) lack of interest in creating new jobs, unauthorized access to classified information and their use in personal / group interests etc.

As the efficient distribution of resources depends on decision-makers, distribution that should be consistent with the objectives defined in the doctrines of national security and defense strategies, the respondents were asked to prioritize the indicators included in the list of risks and threats to national security, because the decision-maker to have an insight into how they perceive the need to allocate resources to prevent and / or counteract their materialization.

Subsequently, after the prioritization of these indicators, respondents were asked that for the top ten risks, threats, vulnerabilities or failures detected, to argue their decision, a similar approach being developed to prioritize the top ten risks, threats, vulnerabilities or failures to national security of Romania in 2020 (as an exercise of projection and forecasting).

It was not a coincidence that the year 2020 was elected. The 241 respondents were selected from among university students in master programs in Bucharest, that have as previously mentioned, the objective of promoting the security culture within the civil society and the training of specialists in the field of national security studies, defense and intelligence analysis.

The reason for choosing the year 2020 to formulate projections and forecasts of the evolution of risks, threats, vulnerabilities or malfunctions to the national security of Romania is the fact that these students are a valuable human resource, which, within six seven years after graduation (i.e. 2020) could become professionals specializing and acting in issues of national security of Romania. This argument is supported by analyzing the distribution of respondents by age, which indicates that 76.54 % of them are ranging from 22 to 30 years.

An additional argument about the usefulness of this research is the fact that, although the master degree programs are designed especially to promote the security culture within the civil society, the distribution of the respondents by field of activity indicate that a percentage of 52.67% of them are coming from the national security, defense and law enforcement structures of our country, whose motivation to pursue these courses is the completion of educational training.

Among them, a percentage of 80.5% is in the age group of 22-30 years, i.e. those individuals from within the national security, defense and law enforcement structures of our country that by the year 2020 will reach their professional maturity.

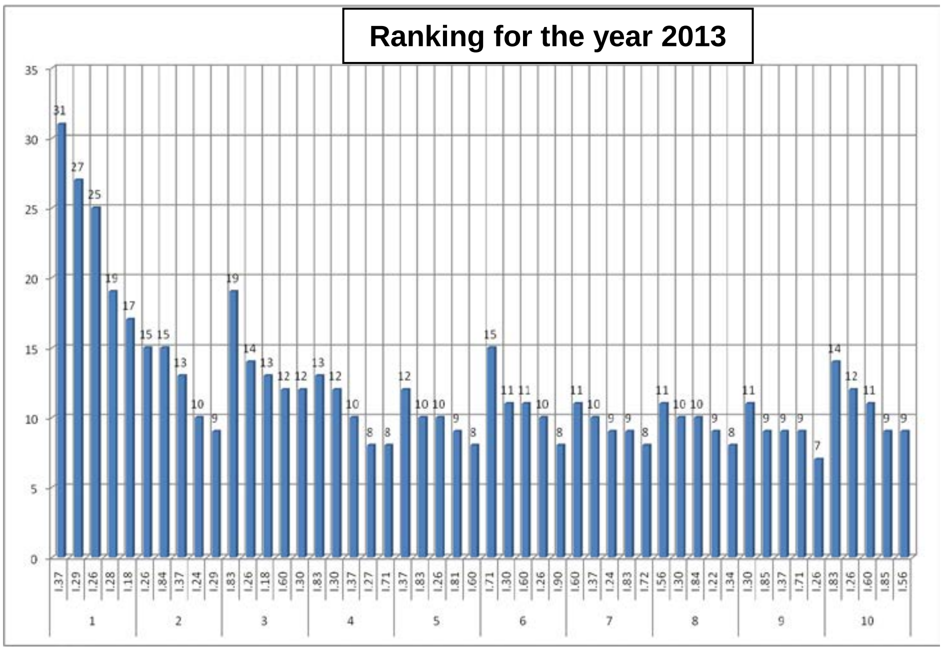
The fact that the distribution of the respondents within the activity fields is balanced (128 of them activating, as previously mentioned, in the structures of national security, defense and law enforcement, the other 113 coming from the civil society) gives a warranty regarding the existence of a balance between the views of experts in the field and representatives of civil society (those civil society representatives who show interest in promoting the security culture).

We are mentioning that although the questionnaire was applied to a percentage that represents about 50% of students in the category mentioned, within the academic environment from Bucharest at that time (January-February 2013), we do not claim that this survey is representative at the national level (although BA studies in the field of security and defense is carried out, to our knowledge, only in Cluj Napoca, Sibiu and Iasi, with a relatively small number of students compared to those in Bucharest), and we are focusing on the qualitative aspect.

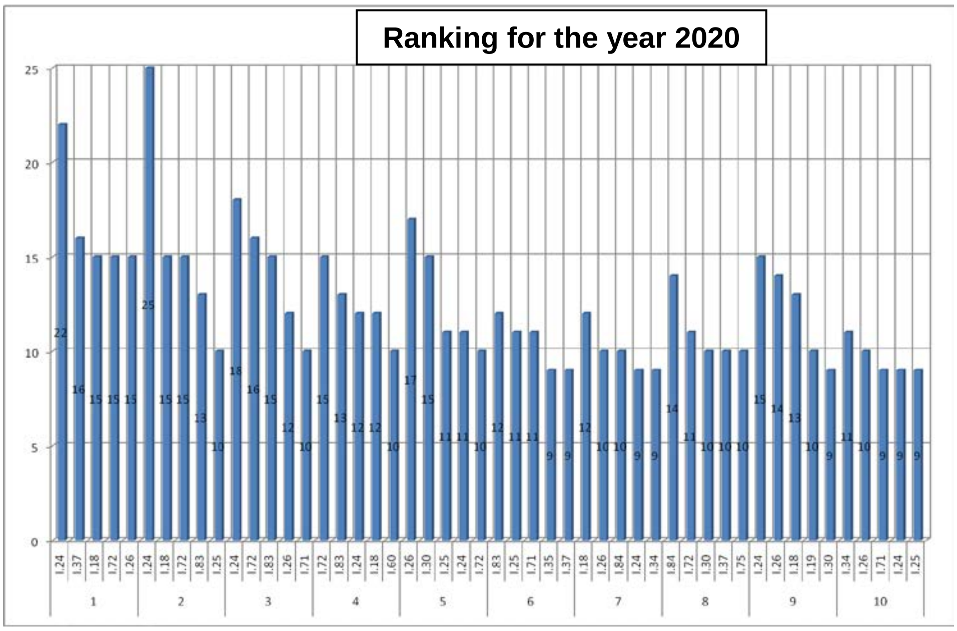
During the analytical phase of the research conducted, the data collected from respondents were subjected to statistical interpretation, tables of values assigned to these indicators are the result of statistical calculations, and this category of data is used to develop the top ten indicators of risks and threats to the national security of Romania. In prioritizing risks and threats we considered that the analytical threshold of at least 5 nominations for each indicator does not affect the results of research, as is the value of just 0.34% (for 2013) and 0.38% (for 2020) of total nominations.

The statistical analysis of the answers given by respondents was done in two stages: in the first stage the rankings of indicators were drawn by levels, from 1st to 10th place for the year 2013 and for the year 2020, taking into consideration the frequency of allocation of indicators by the respondents for each of these places, respecting the minimum threshold of five nominations.

If you were to put together a ranking of the top ten risks and threats to national security, according to the indicators with the highest frequency for each place separately, for 2013, it would include in descending order, only the following seven indicators: I. 37 - corruption among officials of central and local public administration in Romania (1st and 5th place); I.26 - increased social insecurity and the persistence of poverty among the social classes of Romania (2nd place); I.83 - massive migration of the active population capable of work and / or highly specialized (doctors, nurses, engineers, teachers etc.) (3rd , 4th and 10th place); I.71 - human trafficking on or from Romania in order to sustain prostitution or begging networks (6th place); I.60 - espionage activities of the intelligence services of the Russian Federation conducted in Romania (7th), I.56 - trafficking in arms, ammunition and explosives in Romania (8th place) and I.30 - increased crime rate in Romania (9th place).

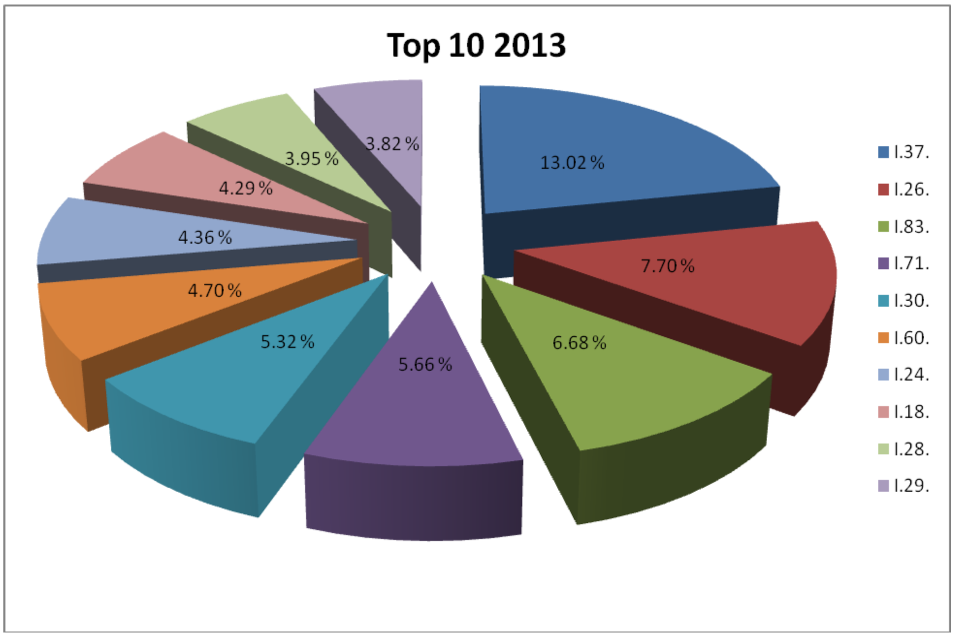

Ranking for the year 2013

When drawing up the ranking for the year 2020 taking into consideration the indicators with the highest frequency for each place separately, it would include, in descending order, the following seven risks and threats to national security: I.24 – the dependence on some resources (gas , energy etc.) not present in sufficient proportion in Romania (1st, 2nd, 3rd and 9th place); I.72 - persisting negative demographic trends (declining birthrates and rising death rate) (4th place); I.26 - increased social insecurity and the persistence of poverty among the social classes of Romania (5th place); I.83 - massive migration of the active population capable of work and / or highly specialized (doctors, nurses, engineers, teachers etc.) (6th place); I.18 - serious Geophysical phenomena, weathering or associated (floods, earthquakes, landslides etc.) (7th place); I.84 - lack of effective strategies for protecting the critical infrastructure (hospitals, energy transmission networks etc.) (8th place) and I.34 - increased drug consumtion that affects the health of the population in Romania (10th place).


Ranking for the year 2020

A quantitative analysis of the frequencies indicates a multiple presence of the indicators in the two tables above, on different levels and with different frequencies (one example being indicators I.83 and I.37, on the final ranking for the year 2013 or the indicator I.24 on the final ranking for the year 2020).

For this reason, in a second phase of the prioritization we have made a frequency weighting for the indicators that respondents have attributed to the final ten places of the ranking for the year 2013 and for the year 2020, thus establishing the indicators frequencies on one of the 10 places in the rankings, resulting in the following prioritization of risks and threats to national security, according to the this weighted frequencies:



According to the ranking of frequencies weighted for the year 2013, the first ten places are occupied by the following risks, threats, vulnerabilities and disruptions to national security:

I.37. corruption among officials of central and local public administration in Romania

I.26. increasing social insecurity and the persistence of poverty among the social classes in Romania

I.83. massive migration of the active population capable of work and / or highly specialized (doctors, nurses, engineers, teachers etc.)

I.71. human trafficking and / or in Romania to sustain prostitution or begging networks

I.30. increasing crime rate in Romania

I.60. espionage activities of the intelligence services of the Russian Federation carried out in Romania

I.24. dependence on some resources (gas, energy etc.) not present in sufficient proportion in Romania

I.18. Geophysical phenomena, weathering or associated (floods, earthquakes, landslides, etc.)

I.28. irresponsible and inefficient exercise of power by political actors in Romania, in disagreement with the principles of democracy and human rights requirements

I.29. terrorist attacks carried out on Romanian territory by elements affiliated with Al Qaeda because of the participation of the Romanian troops in the theaters of operations in Afghanistan;

We can see that of ten top positions of the ranking, only two are related to risks and threats generated by external actors, the 6th place being ranked the risk generated by the espionage activities carried out in Romania by the intelligence services of the Russian Federation, and on the 10th place the threat spectrum of the terrorist attacks committed in Romania by elements affiliated with al Qaeda, because of the participation of Romanian troops in the theaters of operations in Afghanistan. On the 7th place in the ranking is to be found the vulnerability caused by dependence on some natural resources (gas, energy etc.) not present in sufficient proportion Romania, a vulnerability that can turn into threat to national security in the event of some hostile actions against Romania carried out by the Russian Federation, the resource dependence manifested especially with regard to natural gas imported in a certain percentage from this country.

According to the ranking, other risks, threats, vulnerabilities or malfunctions to the national security of Romania are those generated by the actions or inactions of some internal actors: corruption, irresponsible and inefficient exercise of power, social insecurity, poverty, massive migration of the active population, traffic of human beings, criminal activities, serious geophysical phenomena weathering or related to that, which can be found in the strategic documents depicted as risks and threats arising from poor governance, ineffective management of public affairs and proliferation of organized crime activities, i.e. those risks and threats whose appearance or manifestation can be controlled through the implementation of effective public policies and strategies.

Note that the concern regarding the citizen security, which is an integral component of national security in relation to risks, threats, vulnerabilities and failures that can be caused by poor governance or ineffective management of public affairs, can be identified even in the title of two strategic documents that led to the listing of indicators subject to the prioritization by respondents. Thus, in the title of the National Security Strategy are found key concepts such as "good life," "a democratic, secure and prosperous country" and the National Defense Strategy "ensures the security and prosperity of future generations."

According to that document, security and prosperity are the terms of the same equation whose solutions are, among others, the radical modernization of the education system and the effective use of human capital, scientific and technological potential; increase citizens' welfare, health and living standards of the population, and the affirmation and protection of culture, national identity and spiritual life.

These objectives can be achieved only by operationalizing the concept of "good governance", a prerequisite to security and prosperity, the measure unit by which social life validates cumulative result of democratic elections, proves the realism of the political forces ability to fulfill promises in strict compliance with democratic standards, evaluating the success of measures to combat insecurity, inequality and poverty and establish the necessary corrections.

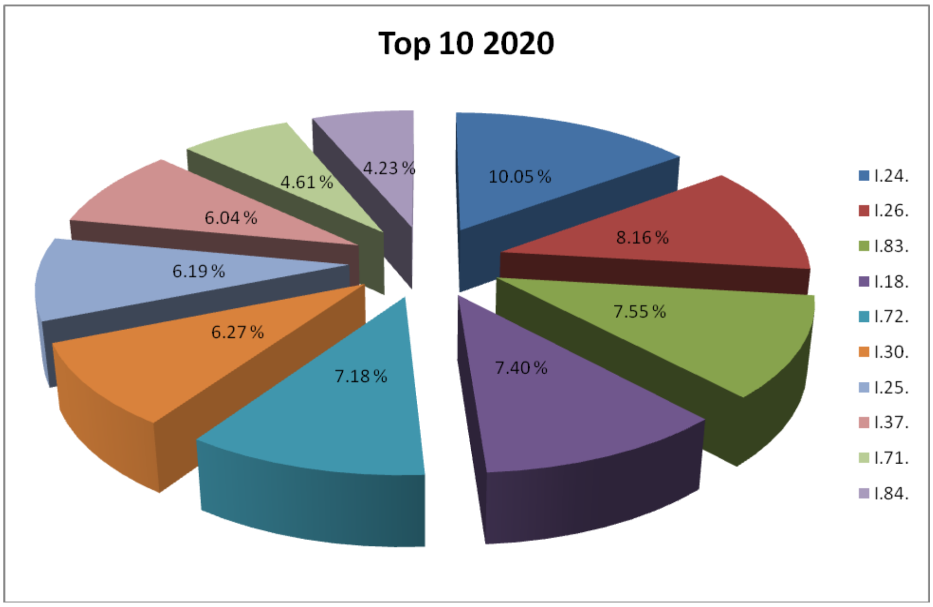
According to the above mentioned strategic documents, "good governance" can only be achieved through an efficient public administration, strengthening the independence and efficiency of justice and increase public confidence in the judiciary system, and increasing the competitiveness and performance of economic and social activity by providing access of all citizens to quality education, radically improved the health of the population and creating a new social balance through a solidarity system able to guarantee the economic, social and health of all participants in the process.

Regarding the ranking of the frequencies weighted for the year 2020, we can notice that the hierarchy of the frequencies weighted with the minimum threshold of five nominations, in descending order, offers us a somewhat similar ranking to the year 2013, in the top ten ranking positions only the vulnerability caused by dependence on some natural resources (gas, energy etc.) not present in sufficient proportion Romania, ranked in the 1st place, being mentioned by respondents as being able to threaten the national security of Romania from abroad.

All the other risks, threats, vulnerabilities or malfunctions to the national security of Romania are those generated by actions or inactions of internal actors, some of them, such as corruption, social insecurity, poverty, massive migration of the active population, human trafficking, crime, serious geophysical phenomena are perpetuating for the year 2020, according to the views of respondents.

In addition, in the top ten places in the rankings were mentioned, still within the type of vulnerabilities or malfunctions which may or have become a catalyst of risks and threats to national security: persisting negative demographic trends (decrease rate birth and increased mortality), environmental degradation due to dangerous, harmful or irresponsible human activities (serious pollution, pandemics etc.), and the lack of effective strategies for protecting critical infrastructure (hospitals, networks for energy transportation etc.).

Also, the lack of effective strategies for protecting critical infrastructure (hospitals, energy transportation networks etc.), which came in 10th place ranking in 2020, ranks in the 11th place in the ranking for 2013, while the risk to national security caused by espionage activities carried out by the intelligence services of the Russian Federation in Romania conducted a "down fall" from the 6th to 11th place, indicator followed by another threat coming from an external actor, namely Iran whose military nuclear program could become operational by 2020, the respondents considering there is a risk that this arsenal will be directed against NATO member states.



I.24. dependence on some natural resources (gas, energy etc.) not present in sufficient proportion Romania.

I.26. increasing social insecurity and the persistence of poverty among the social classes in Romania.

I.83. massive migration of the active population capable of work and / or highly specialized (doctors, nurses, engineers, teachers, etc.).

I.18. Geophysical phenomena, weathering or associated (floods, earthquakes, landslides, etc.).

I.72. persisting negative demographic trends (declining birthrates and rising death rate).

I.30. increasing crime rate in Romania

I.25. environmental degradation due to dangerous, harmful or irresponsible human activities (serious pollution, pandemics etc.).

I.37. corruption among officials of central and local public administration in Romania.

I.71. human trafficking on and / or within Romania, to sustain prostitution or begging networks.

I.84. lack of effective strategies for protecting the critical infrastructure (hospitals, energy transportation networks etc.).

Looking to the year 2020, we believe that respondents are either skeptical about how those risks and threats to national security will evolve, which were classified in 2013 and whose manifestation could be tackled through the implementation of public policies and strategies the next seven years, or consider that these risks and threats have a chronic character, so whatever the action taken by relevant institutions in the field, they will perpetuate for the year 2020.

The appearance in the 2020 ranking of risks, threats and vulnerabilities generated by internal actors, such as persistent negative demographic trends, environmental degradation due to dangerous, harmful or irresponsible human activities (serious pollution, pandemics etc.), and the lack of effective strategies for protecting critical infrastructure, is showing to us that the respondents are aware that ineffective implementation of public policies and strategies to discourage massive labor migration, corruption, human trafficking, crime, drugs consumption that affect the health of the population in Romania or policies for preventing or managing serious geophysical phenomena (pollution from industrial operators) will only lead to greater problems (which were reported by respondents in 2013) and to the emergence of risks, threats and vulnerabilities associated (which appeared on the first positions of the ranking for 2020).

Regarding the development or perpetuation of risks and threats from external actors, the fact that the Russian Federation is, according to the respondents, a vector of threat to the national security of Romania, both in 2013 and 2020, can be explained by the historic "heritage" which the Soviet Union has left to Romania, which correlated with the concern expressed by respondents to the dependence on some natural resources (to be read: Russian gas) not present in a sufficient share in Romania and imported at a price unreasonably high and discretionary established by the Russian Federation. Also the "energy blackmail" is a commonly used weapon by the Russian Federation, especially when winter is coming and when this vulnerability correlates with risk and internal threats caused by social insecurity, poverty and corruption.

In a case of a threat from Iran, positioned on the 12th in the 2020 ranking of the risk that this State to use nuclear potential in order to operationalize an arsenal of mass destruction to be used against NATO member states (Romania inclued) is fueled by the placement of missile shield elements in Deveselu, a decision that provoked intense debate in Romanian and international media.

Instead of conclusions....

We can consider a validation factor of the research conducted that in a survey of "International Brand Consultants", developed under the coordination of the sociologist Vasile Dâncu in November 2008 on a national sample, the question of whether "In Romania, of the following, what are the top three issues that concerns you more? ", the respondents assigned relevant scores of risks and internal threats such as unemployment (first option - 33%, the second option - 8%, the third option - 4%), misery and social exclusion (the first option - 21%, the second option - 13%, the third option - 8%), uncertainty (first option - 18%, the second option - 20%, the third option - 9%), environmental degradation (first option - 6%, the second option - 14%, the third option - 11%), climate change and drug addiction - alcoholism, drugs (the first option - 1%, the second option - 5%, the third option - 14%) , from the external risks and threats only terrorism (first option - 5%, the second option - 8%, the third option - 4%).

Vasile Dâncu explains the results of the survey mentioned in that risk perception in the Romanian society (and more!) is influenced by the uncertainty of tomorrow and the precariousness of the social environment in which respondents live their lives everyday, elements beyond the major risks to Romania, a kind of "hyperpersonalization of the security state". In his opinion, unemployment, poverty and uncertainty of tomorrow (through their personal relevance) "hide" the potential risk of terrorism or the threat of chemical attacks.

A similarity in terms of the persistence of high frequencies assigned by respondents in our research, both in the ranking for 2013 and in the one made for the year 2020 for vulnerabilities caused by serious geophysical phenomena, climate change or the lack of effective strategies protecting critical infrastructure (hospitals, energy transportation networks etc.) or environmental degradation can be seen in how the survey respondents answered the question above "Do you trust Romanian authorities regarding their actions for the protection of citizens in the following areas? " chemical facilities (no - 53% yes - 31%), nuclear power (no - 50% yes - 33%), transportation of hazardous materials (no - 52% yes - 33%), municipal waste incinerators (no - 57% yes - 28%) or floods (no - 50% yes - 29%).

In our opinion, these percentages indicate that the respondents do not feel protected by policies and strategies to prevent or combat the effects of these risks and threats, adopted by the empowered decision-makers[8].

This relationship between the results of two sociological research, conducted at a distance of five years of each other, allows us to say that investigations of this kind can be a tool for feedback and predictability and foresight for decision makers, on how the risks, threats, vulnerabilities and failures to the national security of Romania, as they are mentioned in the strategic documents prepared by analysts in the field is reflected in perceptions of civil society about the work of the institutions in the national security system, defense and law enforcement structures in our country.

In this context, we note that a secondary objective of our research was to provide decision makers a set of indicators (those respondents have mentioned in the prioritization done, other than the 99 indicators listed to be prioritized) and conduct an indirect analysis of how the population is regarding the missions of the institutions of the national security, defense and law enforcement system in our country, based on risks, threats, vulnerabilities and shortcomings on national security stipulated on strategic documents above mentioned.

Finally, a prioritization of risks, threats, vulnerabilities and disruptions to the national security of Romania, as shown in the top of indicators for 2020, may underpin the design of strategic documents for this time horizon (if policy makers considers necessary and appropriate to do so).

References

[1] John Ward, Griffiths, Pat, and Whitmore, Paul, *Strategic Planning for Information Systems,* (New York: John Wiley & Sons, 1990).

[2] J. P. Brans, Vincke Ph., Mareschal B., *How to select and how to rank projects: The PROMETHEE method, European Journal of Operational Research*, no. 24, 1986, pp. 228-238.

[3] J. P. Brans, PH. Vincke, "A preference ranking organisation method, (the promethee Method for multiple criteria decision-making)", *Management science*, vol. 31, no. 6, june 1985.

[4] http://www.promethee-gaia.net/index.html

[5] S. H.Rogers, T. P. Seager, K. H. Gardner, "Combining expert judgment and stakeholder values with PROMETHEE: A case study in contaminated sediments management", in I. Linkov, A. Ramadan, (eds) *Comparative Risk Assessment and Environmental Decision-Making*, (Kluwer Academic Press, Boston, MA, USA, 2004), pp. 305-322.

[6] **** Strategia de Securitate Naţională a României. România Europeană, România Euro-Atlantică: pentru o viaţă mai bună într-o ţară democratică, mai sigură şi prosperă*, 2007, www.presidency.ro

[7] **** Strategia Naţională de Apărare a României. Pentru o Românie care garantează securitatea şi prosperitatea generaţiilor viitoare,* 2010, www.presidency.ro

[8] Vasile Sebastian Dâncu, "Războiul cognitiv, cultura de securitate şi percepţia riscurilor. România şi ceilalţi", în George Cristian Maior (coord.): *Un război al minţii. Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI,* (Bucureşti, Editura RAO, 2010).

"To what Extent is Intelligence Sharing Possible within the Framework of NATO?" An English School Perspective

Adriana SEAGLE[*]

Abstract

NATO is a military alliance sharing more than a common threat. However, when it comes to sharing intelligence the alliance does not have its own intelligence sources except when there are deployments made by NATO. NATO relies on US technologies and other nations for intelligence. Some argue that transforming NATO's system of intelligence of collection, analysis and dissemination is a monumental task requiring the transformation of cultures and mindsets.

The purpose of this paper is to investigate the extent to which sharing intelligence is possible within the framework of NATO, as a regional international society, considering that 'allies' in NATO are former friends and enemies. The international society framework within the English School is a theoretical and empirical concept used to investigate world politics from a society perspective. The framework provides insights regarding rules, norms and practices that states share in the construction of an international society. Inside the English School, NATO is considered a regional international society created by states, 'conscious of common interests and common values who conceive themselves to be bound by a common set of rules in their relations with one another and to share in the working of common institutions'.

Keywords: NATO, intelligence, pluralist, solidarist, regional international society

Introduction

This paper examines the extent to which intelligence sharing is possible within NATO as a regional international society.[1] The topic is timely since most of what has been published in intelligence sharing focuses on intelligence analysis and intelligence organization neglecting states sharing practices within the institutional framework. A recent study using a census sample on two peer reviewed, intelligence publishing journals, reveals that "theoretical" studies in intelligence journals account for only 5 percent, and the majority of articles published in this group focus on "intelligence," "intelligence analysis" and "organizational analysis."[2] Obviously, a significant gap exists in the areas related to ethics and states'

[*] PhD Adjunct Professor, Virginia Tech University, USA

intelligence practices within the intelligence framework. This paper highlights that NATO has intelligence infrastructure but lacks common threat perception and faces technological knowledge hurdles on the use of technology to enhance intelligence cooperation. The paper first introduces the nature and obstacles to intelligence sharing practices within NATO, followed by an overview of the international society approach advanced by the English School (ES). It then investigates the extent to which intelligence sharing is possible within the framework of NATO, conceptualized as a regional international society. Finally, it concludes that intelligence sharing is possible within NATO when states have a common understanding of threat, intelligence and the sharing process.

Overview of NATO's intelligence sharing practices

As a practice in NATO, during the Cold War, intelligence sharing was strategic in nature and focused more on political and military factors including, sporadically, the economic sector. In the contemporary period, the domain of intelligence has shifted to include discussions of terrorism, technological, cultural and economic analysis. Post 9/11, intelligence sharing becomes a demonstration of states' solidarity to prevent common threats as well as a tool of competition between states. Perceived by some as a diplomatic tool for 'better and faster information' and by others as a form of power to achieve a specific purpose within the organization, intelligence gathering and sharing in the post-Cold War era evolved beyond the level of deterrence and retaliation to include the exchange of raw intelligence on non-conventional threats.[3] Studies on NATO's intelligence sharing, and its progress on fighting terrorism, find that multilateral intelligence sharing within the Alliance is impeded first by the complexity of the "terrorism" concept, and then by the structural constraints existing within the system related to different languages, procedures, databases, training and capabilities.[4] For example after 9/11, France and Germany's stance on intelligence cooperation was a priority. However, they emphasised efficiency of human intelligence and fighting 'poverty, humiliation and injustices' as opposed to the US who focused on enhancing technological infrastructure.[5] Belgium, Austria and the Netherlands on the other hand called for the creation of a common European CIA while France suggested that NATO should not spend the energy and resources "recreating methods of action with no real justification."[6]

Research focusing on NATO's intelligence transformation find that despite intelligence reorganization within NATO's *Intelligence Fusion Center*, obstacles remain in areas related to handling, releasing and using timely intelligence.[7] Basically, "all the high and speed won by better communication was lost by political and hierarchical obstacles and more and more commands which wanted to be involved in the process." An insider of Austria Ministry of Defense, reveals for example that intelligence sharing practices within NATO are more divided than united and, "Only SHAPE and some high staff of NATO are truly *joint*."[8] Politicization, political relationship between countries, the nature of contemporary threats, lack of coordination and rotation of experts, different computer software in NATO and member states, lack of mutual trust and states' tendencies to keep intelligence "in house," supplemented by the US monopoly over leadership and technology impede the flow of intelligence sharing within NATO. Consequently, this paper will show that some of the obstacles can be attenuated if a common understanding among parties exists over the threat, its intent, current and future prospects. Within NATO, the practice of intelligence sharing begins at the national level with the collection of information, and is exchanged thereafter, with NATO security agencies or "sister services." Notably, the "exchange'' or flow of intelligence sharing is influenced by NATO's architectural design and culture. From a distance, NATO's intelligence architecture resembles a supranational security, military-based intelligence apparatus assessed by some insiders as dominated by US thinking, dysfunctional, and understaffed.[9]

Fragmentation, decentralization and lack of a common sharing culture are among the weaknesses of NATO's intelligence sharing practices. While improvements in the organizational structure has been made and the culture of cooperation evolved to transform intelligence from the classic Cold War espionage into military intelligence analysis, it is unclear the extent to which the sharing mechanism integrates coherently members of the Alliance into the system, or whether or not state agencies compete with each other for influence and on what grounds. The ES framework of international society can help scholars and intelligence practitioners understand the complexity of intelligence sharing since the concept of 'society' is able to reveal meanings and values of the actors within the system, and subsequently show how and why states engage in intelligence sharing, when the solidarist and pluralist ideas of society are applied.

Within ES, NATO is treated as a regional society or security community with regional ties within the European regional international society, and global ties in US and Canadian membership.[10] As a security community NATO is rooted on military and political integration co-existing within a set of common institutions in which Allies share common values and interests pertaining to security. Furthermore, NATO is a subglobal or a regional international society with *gemeinschaft* and *gessellschaft* (thick and thin) elements of society which, in ES context, remains under investigated generally and particularly in the area related to practices of intelligence sharing. Despite the focus on the global level, ES scholars argue that subglobal international societies are important to investigate because of their expansion into the contemporary global international society and their ability to disclose the creation and share of common norms and rules between countries.[11] Intelligence, as Robert Clark suggested, "is a team sport." And, "effective teams require cohesion, formal and informal communication, cooperation, shared mental models and similar knowledge structures because, without such a common process, any team dealing with complex problems will quickly fall apart."[12]

NATO's approach to intelligence sharing is visible in its organizational transformation. Since 9/11, NATO has sought to increase its multilateral consultation on terrorism and terrorism related issues with the Allies and Non-Allied countries. In 2002, at the Prague Summit, NATO identified intelligence sharing as a tool of cooperation among Allies."[13] And, it took three major steps in reforming intelligence sharing in areas related to collection, analysis, dissemination, and organization. The transformational process focused first on creation, and subsequently on fusion, and consolidation. In the first phase (2003), NATO created the *Terrorist Threat Intelligence Unit* (TTIU), an agency charged with assessing the terrorist challenges, risks and threats to NATO and its Allies. In the second phase (2004), after the Istanbul Summit, NATO enhanced intelligence sharing at SHAPE in Mons, Belgium through the establishment of the Euro-Atlantic Partnership Council/Partnership for Peace (EAPC/PfP) *Intelligence Liaison Unit*, and an *Intelligence Liaison Unit* (ILU) at NATO Headquarters in Brussels. In the third phase (2010-2011), NATO consolidated and enhanced intelligence sharing by setting up the *Intelligence Fusion Center* (IFC) in Molesworth, UK to take over the TTIU's functions and produce intelligence that supports military planning at the operational level and enhance cooperation between NATO civilian and military intelligence. Intelligence sharing as a common practice within an organizational framework however, requires more investigation.

Linking the ES framework with the case of NATO is fascinating not only because NATO is a regional international society with thick and thin elements of society and will enhance the ES view on society, but also because intelligence sharing practices will reveal insights of what states share, how they share, and when they share issues of common interest. This will provide clues therefore, to when and how NATO is a regional society with solidarist and pluralist elements.

The idea of international society through the framework of NATO

According to the definition provided by Hedley Bull, an international society is purposefully created by states who share common norms, values and cultures and who participate in the creation of common rules and institutions. An international society exists:

> *(...) when a group of states, conscious of certain common interests and common values, form a society in the sense that they conceive themselves to be bound by a common set of rules in their relations with one another, and share in the working of common institutions (Bull 1977:13).*

The later revised definition advanced by Bull and Watson (1984:1) suggests that an international society comes into being when:

(...) a group of states...which not merely form a system, in the sense that the behavior of each is necessary factors in the calculations of the others, but also have established by dialogue and consent common rules and institutions for the conduct of their relations, and recognize their common interests in maintaining these arrangements.

As did the European international society when building its identity in relation to the Ottomans, NATO constructed its identity distinct of the Soviet Union and communism accepting members into the Alliance based on their willingness to enhance peace and security. Henceforth, states consented to be bound by a common set of rules in the working of common institutions. A quick glance at the noted definitions may prompt one to suggest that they are similar, however, they are not.[14] In the former, the notion of society is based on "conscious understanding" of interests and values, while in the latter, society is established by "dialogue and consent" meaning that NATO's society can alternate between variants of system and society. At its core however, the study of international society is not sufficiently developed to show which definition of international society accounts for solidarist or pluralist elements of society created by states through their interactions. Some argue that the former definition exhibits solidarist tendencies while the latter is pluralist. Through its practices, NATO may be able to illuminate the ES dilemma of how sharing intelligence constitutes a "society" or an "institution of society" at the regional level.

The degree of institutional sharing and common understanding distinguish international societies into pluralist and solidarist societies. A pluralist form of international society reflects mutual recognition of sovereignty and minimalist rules, understandings and institutions. A solidarist international society shows evidence of solidarity in conceiving common interests. The interests of the whole are central to this form of society. There is more cooperation to safeguard peace and security, share intelligence and sustain common values. Pluralism, "emphasizes separateness while solidarism integration."[15] Scholars focusing on the distinction between pluralist and solidarist international societies argue that the debate between pluralist (functional society - counterbalances between chaos and disorder), and solidarist society (shares norms, rules and institutions) occurs at the border between international and world society in the area of respect and enforcement of international law.[16] Will NATO uphold this distinction? As a regional society organized on the principles of solidarity for security against potential aggressors, it will be interesting to identify the extent to which solidarity is reflected in the framework of intelligence sharing. What counts as security and what counts as a threat? Who decides in NATO what is a threat, and what the intelligence or security is to combat that threat?

In addition to the "sharing" concept derived from the definition of international society, the "conscious" concept has the potential to show the interplay between pluralism and solidarism at the subglobal level. Some scholars recommend, when assessing whether or not states establish a regional solidarist society, to investigate the "consciousness of common interests and values, which is essential in the formulation of rules and the creation of common institutions."[17] Others disagree with the approach on grounds that it is problematic to reach to the "consciousness" of others.[18] ES methodologists recommend to look at ideas recognized by individuals into a society to get to their consciousness. "Paying close attention to the language of the actors and to the way they explain and justify their actions (...) look into the statements and speeches of political leaders, in interviews to elicit the self-conceptions of what the actors are doing."[19] In the context of NATO, this means to investigate whether or not all members of the Alliance have a common understanding of "intelligence" and what the "intelligence sharing" process concretely means.

Establishing a common meaning of what is to be shared, in this case, intelligence, has the potential to enhance the process of sharing. Scholars focusing on the meaning of the intelligence argue, for example, that new democracies experience difficulty in associating a common meaning to the word "intelligence."[20] Except in countries who share English and a common vision to the world, intelligence means different things to different people and different countries. If in Portugal, intelligence remains related to information, in Romania, intelligence relates to knowledge and mind, translated in individual's intellect and cleverness. While in Bulgaria, it remains a word associated with investigation. On the note of "common meaning," it was only recently that in Romania intelligence has been included in the vocabulary to relate to information agencies, secret information and spying. As implied, common language, historical experience, and common culture facilitate a better cohesion of the "intelligence meaning" when it comes for example to the 'Five Eyes' versus the new democracies in Central and Eastern Europe.

In context of "shared meaning" the theory of international society extrapolates that, however NATO members understand the concept of "intelligence" and the process of "intelligence sharing," they will act upon it to participate in the construction of common institutions to improve the common interest, in this sense, intelligence sharing. Therefore, it is no surprise why the US and the UK are leaders in the field of NATO's intelligence transformation. As intelligence is the first line of defense against terrorism, countries seem to work together to create common meanings in the work of common institutions. In the ES sense, a regional society satisfies the following conditions: "community like aspirations, acknowledgement of interdependence, a minimum degree of shared regional identity, defines and assigns roles to play within the region, physical proximity for interaction, a complementing way to assess each other's efforts toward the same end, and legitimately recognized material aspirations."[21] To what extent this is illustrated by NATO remains an object of investigation.

It is known that NATO countries use their national intelligence to support their strategic goals, and that intelligence sharing is a means to achieve those goals through consultation and consensus. In Article 4, NATO Allies pledged to "consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened" while in Article 5, they agreed "that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." The nonconventional threats however, call for placing emphasis more on consultations since "Article 4 provides an opportunity to share information, promotes a convergence of views, avoids unpleasant surprises, and clears a path for successful action-whether that action is diplomatic, precautionary, remedial, or coercive in nature".[22] Notably, consultation and intelligence sharing are conceptualized at the juncture between technology and terror. NATO seems to have evolved from a pure military defense Alliance to an Alliance of dialogue and cooperation, which subscribes to the second definition of international society.

As a regional society with global ties NATO has the potential to underscore the elements of interplay between regional, international, and global international society. Theoretically, the interplay boundary is unclear in ES. Some scholars argue that the interplay is marked, not by lesser cultural cohesion, universal values or dichotomization of society and community, but by an unclear understanding of the boundary of where international society stops, and world society begins.[23] In general, the boundary in the case of NATO is drawn by membership and access to the intelligence sharing framework. For example, NATO's Partnership for Peace (PfP) share some aspects of intelligence with countries in the "waiting room." Recent research on NATO's interaction with non-NATO entities, shows that more simplification in how the information is shared will enhance partnering and will improve the timing and response in future operations.[24] In particular, the scale and system of reference (membership) illustrate a difference between intelligence sharing and access at the regional and global levels. However, in the context of intelligence sharing, access to intelligence seems to be made in relationship to threats. What threats engage the Allies to intensify practices of intelligence sharing?

If in subglobal societies the referent of intelligence sharing is a NATO member, in global international/world society, this is either a NATO member (US or Canada), a non-NATO member or a transnational actor. In practices of intelligence sharing, what else in particular draws the boundary between regional and global? It is important to note, that 'society' and 'community' are characteristics of the global respectively regional levels.[25] According to Barry Buzan, during the Cold War, regional societies were polarized into competing camps but they found ways to coexist through sharing of norms, rules, and institutions (i.e., NATO, EU, OSCE, etc.). In this case, it will be interesting to observe the interplay between subglobal and global as NATO claims to base its coexistence on principles of trust, unity, and coordination for peace and security.

An established argument in the ES suggests that an international society emerges in line with the logic of culture (the civilizational model) or according to the logic of anarchy (the functional model). Empirically, international society evolved to include unity by a common culture, values and interests. Or unity by a shared language, common literacy and artistic tradition. NATO evolved in this sense to include friends and enemies in unity based on common interests to peace and a common fight against contemporary threats. However, do all NATO members have a common understanding of what the common threat is or a common approach to deal with the threat? Empirically, this paper is expected to provide some clues. The Christian international society for example shared a moral culture or a set of common values reinforcing the units' common interests, as did the European international society of the eighteenth and nineteenth centuries, who shared a diplomatic, international political culture. Some scholars argue that the logic of culture has determined the degree of states' integration into international society, but the logic of anarchy brought states into international society.[26] For example, the accession of Greece and Turkey in 1952 was facilitated by the Korean War while the integration of Eastern and Central Europe by the end of the Cold War. Through enlargement, the Alliance evolved to an Euro-Atlantic mentality to include peace and security not only for the North-Atlantic, but also for the Eastern and Central European Neighborhood. How is intelligence sharing reflected in this unity? Is there a distinction between old and new friends, friends and enemies, core and periphery? Two distinctive features of international society are unity and coherence when it comes to power, common interests, and values. On the other hand, consensus describes the agreed framework of rules and institutions by NATO members, while coherence reflects the degree of shared values or the shared framework of a common understanding. Nevertheless, leading ES scholars argue that the limited rules of coexistence are an indicator of a society in decline.

NATO intelligence sharing practices – evidence of solidarism and pluralism

Academics and policy makers refer to the 21st century as the "Pacific Century" when US strategic interests have shifted from Europe into China, N. Korea and Iran. Budget cuts in the US military and lack of capability gaps in intelligence, surveillance and reconnaissance assets of the European Allies prompted US official, Robert Gates to declare one day that "Europe may no longer be worth defending" because, Europe is unwilling to pay for its own defense. According to Gates, "at times, NATO has struggled to sustain a deployment of 25,000 to 40,000 troops, not just in boots on the ground, but in crucial support assets, such as helicopters, transport aircraft maintenance, intelligence, surveillance and reconnaissance."[27] In his view, the transatlantic gap in defense spending, and the lack of political will of government officials will hamper NATO's military missions.

Considering how members of the Alliance approached the war in Iraq and Afghanistan it seems that consensus within the Alliance over how to conceptualize the vital common interest, and provide for security is difficult to reach. For example, in the context of Afghanistan, Germany restricted its troops from using lethal force, which prevented their deployment in combat against the Taliban. Changing government in the Netherlands resulted in a sudden withdrawal of troops, and changing government in Romania raised concerns over budget, deaths and serious injuries of Romanian soldiers prompting discussions of an 890 troop withdrawal from Iraq.[28] Similar discussions extended to Lithuania, Italy, and other NATO members. Gates stated publicly that NATO lacked intelligence, surveillance and reconnaissance assets making the most advanced European fighter jets useless. NATO responded to Gates' concerns with the "smart defense" approach making aerial refueling a strategic priority, and applying the principle of pooling and sharing of military resources on capabilities and procurement. Up to this point, NATO members relied on US leadership and technological assets to coordinate offensives.[29] In the defense industry, Gates is known to advocate "strategy over procurement,"[30] and relevant to consider here is the compatibility of technology while addressing current threats as well as the ability of current technology to win peace (hearts and minds) of existing threats.

The purpose of intelligence is to assist decision-makers in areas where immediate action is needed.[31] A study released in 2006 found that "NATO Headquarters had limited mandate or capabilities for intelligence gathering except when there are deployments of NATO or NATO led forces. For intelligence, NATO depends on nations, which then share it as appropriate, with Partnership for Peace (PfP) partners, and other countries contributing forces to NATO-led operations in PfP activities."[32] As suggested, intelligence is "the world of secrets" which can be shared or strategically kept from friends in attempts to construct one's identity or consolidate its position within the Alliance. Historically, the relationship between the US, France, and UK regarding intelligence sharing, especially during the Cold War, has not been one of trust and mutual cooperation. The mistrust that NATO allies had in the American deterrent strategy was not related to the fact that America might not be able to keep its commitment to defend European allies but to the idea that in an event involving nuclear weapons "an American politician would never exchange the survival of Detroit for that of Paris."[33] A psychological impact prompting De Gaulle, in 1966, to withdraw French forces from NATO and demand that NATO's headquarters be moved from Paris to Brussels. Notably, France's reaction was based on the US's refusal to share control over technological intelligence and nuclear weapons, as well as the fact that during the Cuban Missile crisis "America's allies from Western Europe were being *informed* rather than *consulted*" as required by Article 5.[34]

Past practices of intelligence sharing indicate that NATO's anxiety about intelligence collection and the increase in alerts prompted the development of new technological initiates, resulting by the 1980s, in substantial improvement in satellite development.[35] On the other hand, the flow of intelligence has been much smoother between the US and UK especially in SIGINT, however, outside of SIGINT sharing was selective involving exchange of papers and US participations in the drafting process of the British JIC.[36] In the contemporary period trust among allies remains a concern. For instance, media speculated that the German General Lt. Gen Klaus Schuwirth became the EU's Director of Military Staff in Brussels because of the Americans reluctance to share high-grade signals intelligence with the French.[37] The relationship between France and Britain has also been marked by mistrust as De Gaule, for a long time, viewed Britain as an American asset in NATO.[38] Additionally, it is important to note that after 9/11, NATO intelligence services have been criticized for lack of coordination and inability to connect the intelligence dots on the American hijackers.[39] US Defense Secretary Rumsfeld, for instance, recommended NATO to do better intelligence coordination to address strategic issues before they become military ones.

> NATO would do a better job of seeing that the intelligence capabilities of the respective countries are brought together and that the people in NATO and the capitals of NATO countries are kept tuned into those threats and the kinds of capabilities that we as free people face. We're much more likely to get a faster common understanding to the extent we have a reasonably similar perspective with respect to what the facts are.[40]

Intelligence sharing within NATO is not only affected by matters of coordination but also by the merit of classification despite the fact that NATO promotes common security clearances and common practices for handling intelligence documents. What may be deemed secret or very secret for the UK may be only confidential for Bulgaria and Romania. Belgium for example exchanges intelligence information within their network without classification.[41] This facilitates faster exchange, eliminates the effect of "information constipation," and enhances efficiency and productivity. For example, NATO's Nordic countries (Denmark, Estonia, Iceland, Norway) find cooperation with non-NATO members Finland, and Sweden "natural." "It's a question of geography, culture, and values. We speak the same language. We feel closer to each other than most other people [...] There is already a very good cooperation between intelligence services in the Nordic countries. It was like this even in the Cold War. There are close contacts at a personal level. It's an issue of trust, of joint interests."[42] This is an illustration of tacit intelligence sharing and cooperation. "Do you believe that if there is an attack on one of the Nordic countries, it is possible to isolate that country? No. If one Nordic country is attacked, it may happen that all the others are also involved."[43] The regionalism practice to intelligence sharing is enhanced here by a common understanding of identity, culture, geography and values.

Agreeing over a common definition on terrorism and having a common approach to combat it will enhance intelligence cooperation within NATO. Whereas the US and UK deal with terrorism in the military realm, Allies belonging to the EU address terrorism in the domain of crime and law enforcement. They look at peace and security through a human security, democracy and constructive conflict management perspective. There is no question that central on NATO's Allies intelligence agendas are Islamic terrorism, arms proliferations, criminal organizations, economic and scientific interests. However, when it comes to cyber security for example, Belgian intelligence cooperates with the EU and NATO security bodies when they are targeted by cyber-attacks. But, cyber-attacks are talked about in the context of criminal behavior not a terrorist behavior, thus, not a military concern.[44] The Belgian intelligence chief seems to suggest that a cyber-defense institution in the UK may not be so efficient to defend, for example, NATO's periphery despite the fact that "at the level of international cooperation, exchange of information is very active." He credits this to the inexistence of a centralized body where civilian, military, and the federal police work in tandem to come up with a general definition and a common approach on dealing with cyber threats.

In context of "common threat" and "intelligence sharing," Turkey is relevant to consider, especially when it comes to Iran's nuclear threat. Unlike the US, Turkey refuses to acknowledge Teheran as a regional threat of destabilization and arms race, and instead includes Israel as one of the countries posing a major threat. The US views Turkey as a strategic ally to place a missile defense system to counter the proliferation of ballistic missiles, especially missiles coming from Iran. Turkey interprets the missile system as an enmity instrument to destabilize the region, and fuel the arms race. For instance, in the midst of missile system negotiation, Turkey's Foreign Minister Ahmet Davutoglu, stressed that "We don't see any threat from any of our neighboring countries, whether it is Iran, Russia, Syria or others [...] I stated very clearly that Turkey will not be a frontal or flanking country [of the NATO missile shield] and we do not want to see again a zone of the Cold War and its psychology in our region."[45]

An emerging pattern in the complexity of intelligence sharing is the agreement of a common definition of a threat. While discussions between Ankara and Washington continued over the installation of the two radar systems, Turkey was not sure that this was a matter of providing for security or as a matter to increase dissension in the region. "This is not an issue for NATO now. First, a definition of the threat against NATO members must be made. Then we can consider the issue in this light."[46] Notably, both Allies exhibit interesting practices of intelligence sharing when it comes to their common enemy, the outlawed Kurdistan Workers' Party (PKK). There is no mentality of "if you gain, I lose," but interestingly, the interaction with the US enabled Turkey to deal with PKK with military means.

Nevertheless, relevant data reviewed on the case show that the US decided to share intelligence with Turkey on PKK only when PKK interfered with US interests in Iraq and only when it wanted to prevent a unilateral invasion of Turkey in northern Iraq on grounds of self-defense. Data show that sharing intelligence intensified between the US and Turkey in November 2007, under the Bush administration, when both countries declared the terrorist organization PKK a common enemy.[47] The process of intelligence sharing consisted of allowing the Turkish military personnel to use the predator system and air vehicles with sensors in missions of reconnaissance. "The US military began supplying real-time intelligence to Turkey and Turkish Armed Forces which used the intelligence to launch air strikes against PKK targets in the north of Iraq."[48] Concerns over sharing timely intelligence with Iran facing a terrorist threat from PJAK (the Iranian branch of the PKK) brought the US-Turkey cooperation on intelligence under scrutiny over trust numerous times.[49] Turkey claimed however, that intelligence sharing with Iran is only political and did not reach the level of military generals.[50] The US on the other hand, believed otherwise amassing suspicions that the sharing was strategic and operational.

Intelligence sharing between Turkey and the US continued to the extent that the US showed leadership and trained Turkey on how to use real-time intelligence to avoid friendly fire over northern Iraq with US pilots.[51] The efficiency of the intelligence cooperation came under scrutiny when a Turkish military post was been attacked by 300 PKK terrorists resulting in 17 casualties. As much as this was a NATO intelligence failure, the shortcoming was a failure of the effectiveness of "actionable" intelligence sharing between the US and Turkey. When asked to explain how 300 PKK terrorists were able to cross the border between Iraq and Turkey to attack the post without being caught by US surveillance mechanism, an US official diverted the response.[52] To overcome the failure, the US suggested that Turkey increase communication between two offices allowing the US to adjust the intelligence system. Their friendly relations in intelligence sharing expanded when Turkey requested the US to base predator systems in Turkey.[53] With respect to PKK movements, a common enemy of Turkey and the US, intelligence sharing slowed down and stopped after the US withdrawal from Iraq. The supply of data 24 hours a day in Cyrillic on PKK movements has stopped because of the safety of US pilots flying over the PKK inhabited region.[54] This is an indication that the practice of sharing intelligence within the framework of NATO goes hand in hand with technological power and states individual interests.

Within NATO, Turkey is an ardent advocate for not sharing intelligence with non-NATO countries including Greek Cyprus.[55] In the context of NATO's ballistic missile defense system, Turkey sought numerous assurances from the US and NATO Allies that intelligence gathered using the missile shield's sensors would not be shared with Israel.[56] The relationship between Turkey and Israel goes beyond the Alliance constraints of membership to include bilateral incidents such as the "Israeli military using force against civilians including women and children, and the elderly who wished to take humanitarian aid to Gaza people."[57] Although, Turkey and Israel had a strong strategic bilateral relationship enhanced by arms procurement. Ankara addressed the gap in surveillance satellites buying from Israel 10 Heron Unnamed Aerial Vehicles (UAVs).[58] Intelligence sharing did not go too much beyond that of spy satellites provided by Israel to boost the Turkish military capability to fight PKK.[59] Some Turkey officials argue that a sincere Israeli apology on killing Turkish civilians could mend their relationship. In the meantime, Turkey made a goal of using the issue to block, when presented with the opportunity, Israel's access to NATO's Partnership

Cooperation Menu (PCM) in the Chicago Summit and other critical missions. Notably, as a NATO official stated, “NATO’s Israel relations cannot be restored until Turkey-Israel relations are normalized.”[60] Turkey and Israel’s quarrel reflects geopolitical power and bilateral interests brought within the Alliance’s forum of intelligence sharing by its members.

The US-Turkey case highlights the importance of real-time intelligence, the fragmentation of intelligence when it comes to individual interests, the relevance of cost, innovation, and a different conceptualization of terrorism and terror. Unlike the US, Turkey has been accustomed to living in ethnic terror for quite some time. In the context of intelligence, sharing is nothing more than vital flowing of and timing information toward a source that may use it. Unused intelligence has no value. Improving the flow of intelligence is a critical task for NATO, a voluntary organization of sovereign states who find difficult to volunteer their national intelligence within NATO, first due to technological incompatibility and thereafter from considerations related to the importance of the intelligence as well as countries historical and cultural differences. NATO claims to have a long history of good intelligence sharing practices, and hopes that, though an array of measures, to come to a better understanding of the nature of the terrorist threat advocating that “prevention is more than information sharing.”[61] In the area of prevention, the Alliance invests in technologies and scientific solutions to prevent spectacular acts of suicide bombers in public spaces. Some programs of cooperation includes STANDEX with Russia. Good practices refer to support provided to Allies when hosting high visibility events such as the Athens Olympic Games, the 2006 FIFA World Cup, and meetings of Heads of State and governments.

NATO provides a forum for transatlantic political dialogue and consultations on counter-terrorism for its 28 Allies and increasingly for its partner nations. Today, the Alliance has more than 50 partner nations from around the world. With our partners, we consult and share information, assist with capacity building and joint capability development in areas such as counter-IED or harbor protection. All in all, NATO offers more than 1,600 activities under its partnership programs, including training courses, exercises and seminars in the fight against terrorism.[62]

Member states of the Euro-Atlantic Partnership Council (EAPC) endorsed a plan to fight against terrorism through efforts of information and views sharing related to terrorism, both in EAPC meetings and in seminars and workshops under the auspices of EAPC/PfP.[63] Notably, the plan specifies that lead nations take an initiative to organize meetings. EAPC states EAPC/PfP Intelligence Liaison Unit (ILU) to promote in accordance with their domestic laws, exchange of intelligence relevant to terrorist threats. Note that the mechanism of intelligence sharing within NATO is in flux as are the threats. The establishment of the NATO Centre of Excellence and Defense against Terrorism units help NATO enhance dialogue and scientific cooperation in identifying and mitigating new threats to security.

An important obstacle to information sharing is technology because technology is part of the infrastructure of intelligence sharing. Compatibility in computer technology and better coordination helped NATO-led International Security Assistance Force (ISAF) counter the IED threat in Afghanistan. "Especially in land operations...we have been a coalition that has been divided by our technology...we now stand together as a coalition, joined in our technology" said Georges D'hollander, general manager of NATO's C3 research and development establishment in Hague. Notably, political will is another obstacle to information sharing. Access to information is granted on various levels and it depends on the sensitivity and the will of the country to share. The "smart defense" concept calls for further cooperation and coordination among NATO countries. Nine NATO countries (Canada, France, Germany, Italy, Netherlands, Norway, Spain, Britain and the United States) agreed to share imagery and other information from national assets. "By rapidly sharing imagery, we can avoid having multiple assets deployed in the same location, cover a significantly larger area, or cover a specific area for a longer period. In effect, what we get is more intelligence for our euro."[64]

Intelligence sharing practices with friends and former enemies

How does intelligence sharing occur between older NATO members and new entrants? It is a fact that NATO led military operations require an integrated intelligence sharing structure and although the infrastructure has been created, NATO members remain reticent in sharing national intelligence within the NATO network. Mutual trust in sharing raw intelligence is influenced by political preferences, special relationships, states concerns over misuse of their intelligence, the possibility of being wrong, either by faulty satellite systems, untruthful informers or just states preferring to hold onto information in order to test friendships and reliability of their partners.[65] On intelligence cooperation, General Wesley Clark (former NATO Supreme Commander) stressed that "one has to be very careful of information that is given by any other country's sources. It is a function of the precision of the information, the source of the information, the duration of the relationship, other conflicting methods. It is part of using intelligence to be able to evaluate its credibility."[66] Furthermore, someone else suggested that NATO would benefit from a black box to collect and disseminate intelligence without states knowing who provided the intelligence since, when it comes to intelligence sharing, "we always get into this argument about what we can release to our friends."[67] NATO members agree that they must meet the common threats where they are however, they seem to disagree over how to approach them. In the American realm, the war on terror is framed as "an intelligence problem, a financial problem, a battle of ideas, a problem dealing with ungoverned areas, and a problem of countries providing heaven."[68] While Europeans view it as a result of injustices committed by colonization and underdevelopment, a problem to be dealt with in the justice system thus, outside of the competency of NATO. Schroeder for instance reiterated that "terrorism cannot be fought with arms and police. We must also combat its roots in economic underdevelopment."[69]

Intelligence sharing between Poland and the US, for example, unfolds in the framework of strategic cooperation and bilateral agreements. Both states agree to share information on terrorism and nuclear proliferation within the framework of NATO's Article 3, which emphasizes "separately and jointly." While the US engages in providing "missile defense, situational awareness and information regarding threat assessments associated with US military facilities, assets and personnel present on the territory of Poland," the US appears to lead in intelligence sharing, intending to provide Poland with an avenue process "to request information from the US that pertains to intelligence or warning threat information associated with US military facilities on the territory of Poland."[70] Which indicates that the information sharing between these two countries flows in a process by controlled the US and when the interests of the US are affected. Notably, there is indication that states resort to assuring faster intelligence sharing after they sign contractual agreements (i.e., Belgium and Turkey involving the PKK).[71] France's intelligence sharing with the US intensified after 9/11 and as a French official stated, "we do it quietly. We had to work on our intelligence very hard during the 1990s, when there was a wave of terrorists attacks on French targets from Algerian Islamist. We have the linguists and we have the expertise. And the US knows that."[72] Both France and Germany have been urged by the US to play a bigger role and commit more forces in Afghanistan. It seems that intelligence sharing within NATO is coordinated by the US and facilitated by the US technological infrastructure. France's role in NATO increased after the dispute over the US invasion in Iraq. "If you can't fight them, join them." France agreed to participate in peacekeeping operations training Iraqi police personnel. France pulled its troops out of NATO command in 1966 but remained a NATO member. After 2003, military and intelligence sharing between France and the US intensified. France has been active in peacekeeping missions in Bosnia, Kosovo, and Afghanistan where a French general commanded NATO forces. "We are the second largest contributor in military terms to NATO and the fifth largest in terms of financial support" according to Michelle Alliot-Marie, French Defense Minister. The US sharing intelligence with France intensified with France's 2013 intervention in Mali.

Assessing NATO's solidarist and pluralist practices

NATO has intelligence sharing infrastructure but lacks common threat perceptions and faces technological hurdles on how to use technology to enhance intelligence cooperation. Within NATO, the Allies acknowledge the norm of "need to share" intelligence, technology, and methods of surveillance in countering contemporary threats. They share the importance of intelligence coordination, and the need to assess threats and consider common responses. Membership and access to intelligence are norms guiding the sharing process. Considering the experience in Iraq and Afghanistan, NATO members display concerns of better unity, coherence, respect and international law enforcement. Security is valued, but threats to mutual security are not viewed with the same intensity by all members of the Alliance. NATO's intelligence is shared bilaterally and multilaterally however, national interests still govern states' behaviors. When sharing intelligence there is a fear of compromise and penetration. Threats are conceptualized globally and regionally. There is no common intelligence sharing picture of which threats are global or regional. For example, PKK came to be considered a "common threat" by Turkey and the US in 2007, which makes it a global threat. PJAK, the Iranian branch of PKK has not been viewed in the same light before concerns over Turkey sharing intelligence with Iran on PJAK arose within the US.

The Allies embrace the idea that NATO is a forum of engagement and dialogue. Allies acknowledge US leadership, expertise and technological capability. There are fears related to lack of technology when it comes to acting on intelligence and sharing intelligence using compatible systems, as well as concerns that too much technology, such as the missile defense system, will produce more insecurity and arms races than security. The Allies also share the idea that NATO is united in its solidaristic mission. The union is influenced by the UN mandate to interfere in other sovereignties (i.e., Iraq and the division between new and older democracies). There is evidence that states value sharing capabilities and assets in a common defense system. When it comes to volunteering their national intelligence, the lack of common definitions of threats impedes the flow and quality of information.

Allies do not have a common understanding of threats and the technological ability to monitor and counter the emerging threats. As the case of Turkey shows, there is lack of technological capabilities to share intelligence in, what is supposed to be a critical focus to NATO, the Middle East. Some suggest the need to identify a problem before it becomes a problem. Obviously Turkey demonstrated Alliance solidarity when it agreed to host the missile defense system on its territory.

With respect to solidarist and pluralist societies, NATO is a solidarist society at emphasizing the core mission of the alliance. Intelligence sharing is however, compartmentalized, regionalized, and influenced by common identity, culture and values. Threats are also regionalized and when the US is involved they become global and are dealt with militarily.

There is lack of unity however, at the periphery on how NATO's mission regarding threats should be accomplished. The core formed by older Allies is fragmented over access to intelligence and the existence of the UN mandate whether or not to interfere in other sovereignties. The lasting mistrust between France and the US on the one hand and disunity between Germany, France, UK and the US over the war in Iraq as well as how to use German forces, on the other hand. The claim that "pluralism emphasizes separateness" is evident in how NATO members approach the common interests such as the PKK and terrorism (in military vs. police realms), intelligence sharing mechanisms (the need of a common compatible infrastructure) integrating both civilian and military capabilities, and their reactions over sharing intelligence. Unity is apparent over "the need to have and the need to integrate" however, disunity is visible in the process of "what" to integrate. The interplay between the regional and global scale in intelligence sharing is played in context of membership, access to technology, friend and enmity relationship.

Conclusion

The purpose of this paper was to investigate the extent to which sharing intelligence is possible within the framework of NATO. The findings suggest that NATO has intelligence sharing infrastructure and elements of a solidarist society exist in the urgency or need to have and share intelligence, acquiring technology, the importance of intelligence coordination, sharing capabilities and assets, as well as combating the common threats. The study's highlights are that intelligence sharing within NATO is more than a governing principle, it is a process, a supranational institution in which good practices do not seem visible when things go well. Bad practices however, disclose the shortcomings of the process. Intelligence sharing is regionalized, and fragmented by special interests. In the case of the US and Turkey, the failure of intelligence sharing may be attributed to the idea of a common threat, time, technology, political will, and states national interests. In their intelligence cooperation, both Turkey and the US went beyond the Alliances core mission to provide for their own interests. On the one hand, the US does not want to share intelligence with Turkey because Turkey, in return, may share it with Iran. Consequently, Turkey does not want NATO to share intelligence with Israel, who, in return, will share intelligence with Greek Cyprus.

An important finding of the intelligence sharing process is that now NATO has a form of intelligence sharing infrastructure but it needs a common understanding of threats, intelligence and the sharing process. Consequently, it is the importance of the US in leading, training, reorganizing and coordinating intelligence sharing within NATO. A common definition of threats however, will help NATO identify common approaches to technology innovation and ways to address them. The US role in NATO is paramount. While the US can lead the process, other countries can learn how to lead, train and coordinate to improve the system. A common intelligence sharing infrastructure is critical as is political will to use it. The sharing of intelligence is possible within NATO when Allies have established a common understanding of the threat environment and act on that understanding to create common sharing institutions avoiding duplication and special interests. Intelligence sharing needs a technologized infrastructure invulnerable to cyber-attacks however, as one NATO official suggested, national and international "threat prevention is more than intelligence sharing."

References

[1] In this paper, intelligence is used in the sense of states practices of dissemination, or, "the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who needed."Robert M. Clark, *Intelligence Analysis*, 3rd edition (Washington DC: CQ Press), p. 2; Rob Johnson, *Analytic Culture in the US Intelligence Community* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005), 70.

[2] Miron Varouhakis, "What is being published in Intelligence? A Study of Two Scholarly Journals," *International Journal of Intelligence and Counterintelligence,* Vol. 26, No. 1, 2013, pp. 176-179.

[3] *Reuters*, "NATO launches Afghan intelligence sharing drive." July 15, 2010.

[4] Claudia Bernasconi, "NATO's Fight Against Terrorism: Where Do We Stand?" *NATO Defense College Research Paper* No. 66, April 2011.

[5] *International Herald Tribune,* 'Agencies in EU Nations to Coordinate Terror Fight Actions' 17 March 2004.

[6] Munich Conference on Security Policy, 'Michele Alliot-Marie, French Minister of Defense' 4 February 2006.

[7] Friedrich W. Korkisch, "NATO Gets Better Intelligence," *IAS Reader, Strategy Paper* 1-2010. Available online.

[8] Friedrich W. Korkisch, "NATO Gets Better Intelligence," *IAS Reader, Strategy Paper* 1-2010, pp. 8.

[9] *EU Observer,* "Belgian Intelligence Chief talks to EU Observer." 17 September 2012.

[10] Mark Webber, “NATO: Within and Between European International Society,” *Journal of European Integration*, Vol. 33 Issue 2, pp. 139-158.

[11] Hedley Bull and Adam Watson (eds), *The Expansion of International Society* (Oxford, Clarendon Press, 1984); Adam Watson, *The Evolution of International Society* (Routledge, 1992).

[12] Robert M. Clark, *Intelligence Analysis*, 3rd edition (Washington DC: CQ Press), p. 2; Rob Johnson, *Analytic Culture in the US Intelligence Community* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005), 70.

[13] NATO Multimedia Library, ‘Intelligence Sharing in Combating Terrorism’ http://natolibguides.info/intelligence (Accessed on August 15, 2013).

[14] Yannis Stivachtis, *The Enlargement of International Society* (St. Martin’s Press, Inc., 1998), p. 15.

[15] J. Czaputowicz, “The English School of International Relations and Its Approach to European Integration, ”*Studies and Analyses*, Vol. II, No. 2, 2003, p. 42.

[16] Barry Buzan, *From International to World Society?* (Cambridge University Press, 2004); Nicholas Wheeler, “Pluralist or Solidarist Conceptions of International Society: Bull and Vincent on Humanitarian Intervention” *Millennium*, Vol. 21, No. 3, pp. 463-487.

[17] Mohamed Ayoob, “From Regional System to Regional Society: Exploring Key Variables in the Construction of Regional Order,” *Australian Journal of International Affairs*, Vol. 53, No. 3, 1999, pp. 247-60.

[18] Sheila Grader, “The English School of International Relations; evidence and Evaluation,” *Review of International Studies*, Vol. 14, No. 1, 1988, pp. 29-44; Martha Finnemore, “Exporting the English School?” *Review of International Studies*, Vol. 27, 2001, pp. 509-513.

[19] Cornelia Navari, “What the Classical English School was Trying to Explain, and Why its Members Were not Interested in Causal Explanation,” on Cornelia Navari (ed), *Theorising International Society* (Palgrave Macmillan 2009), pp. 39-57.

[20] Florina Cristina Matei & Thomas C. Bruneau, “Policymakers and Intelligence Reform in New Democracies ”*International Journal of Intelligence and CounterIntelligence*, Vol. 24, No. 4, 2011, pp. 656-691.

[21] Mohamed Ayoob, “From Regional System to Regional Society: Exploring Key Variables in the Construction of Regional Order,” *Australian Journal of International Affairs*, Vol. 53, No. 3, 1999, pp. 247-60.

[22] The *Strategic Concept of 2010*.

[23] Barry Buzan, *From International to World Society?* (Cambridge University Press, 2004), p. 18.

[24] NATO Joint Analysis & Lessons Learned Center, “Information Sharing With Non-NATO Entities,” Report Published on 13 November 2012; JALLC - Joint Analysis and Lessons Learned Centre, Lisbon, Portugal (Accessed on August 14, 2013).

[25] Barry Buzan, *op. cit.*, p. 45.

[26] Yannis Stivachtis, *The Enlargement of International Society* (St. Martin’s Press, Inc., 1998), p. 15.

[27] *EU Observer*, “US Defense Chief: Europe may no longer be worth defending,” 10 June 2011.

[28] *Washington Post*, “Romanian PM Proposes Pulling Iraq Troops,” June 29, 2006.

[29] *EU Observer,* "EU countries to reduce dependence on US military," 23 March 2012.
[30] US Department of Defense, "Gates Unveils Strategy to Cut Costs, Boost Efficiency," September 14, 2010.
[31] Richard Clark, *Intelligence Analysis: A Target Centric Approach.* Third Edition (CQ Press, 2010); Loch, K. Johnson and James, J. Wirtz (eds), *Intelligence: The Secret World of Spies: An Anthology*. Third Edition (Oxford University Press, 2011).
[32] John Kriendler, "NATO Intelligence and Early Warning," *Conflict Studies Research Centre,* Special Series 2006/13, p.2.
[33] Richard Garwin and Georges, Charpak, *Megawatts and Megatons: The Future of Nuclear Weapons* (The University of Chicago Press, 2002), p. 369.
[34] Richard J. Barnet and Marcus G. Raskin, *After 20 Years: The Decline of NATO And the Search for a New Policy in Europe* (Alfred A. Knopf, Inc., 1966), p. 54.
[35] R. Aldrich, "Intelligence within BAOR and NATO's Northern Army Group," *The Journal of Strategic Studies,* Vol. 31, No. 1, 2008, 89-122. February Issue.
[36] M. Hermann, M., "Understanding the UK-US Intelligence Partnership," in M. Tuzuner (Ed) *Intelligence Cooperation Practice in the 21st Century: Towards a Culture of Sharing* (IOS Press, 2010) pp. 17-30.
[37] *EU Observer*, "German to lead 'Euro-Army," 17 November 2000.
[38] Toni Blair, "Speech in Warsaw," 6 October 2000 (Available Online).
[39] *EU Observer*, "Total control requires total surveillance," 17 September 2001.
[40] US Department of State, "Rumsfeld Urges NATO Intelligence Coordination," Munich Security Conference, February 7, 2004.
[41] *EU Observer,* "Belgian Intelligence Chief talks to EU Observer," 17 September 2012.
[42] *EU Observer,* "Nordic countries huddle together as world gets bigger," 6 December 2010.
[43] *EU Observer*, "Nordic countries huddle together as world gets bigger," 6 December 2010.
[44] *EU Observer,* "Belgian Intelligence Chief talks to EUObserver," 17 September 2012.
[45] *EU Observer,* "Turkey on collision course with NATO over Iran," 2 November 2010.
[46] *Today's Zaman*, "US seeks to place radar in Turkey as part of missile shield," 8 February 2010.
[47] *The Anatolia News Agency,* "Turkey and US continue intelligence sharing properly," 25 June 2010.
[48] *The Anatolia News Agency*, "US Ambassador denies deficiency in intelligence sharing," 21 June 2010.
[49] *Today's Zaman*, "Turkey assures US over intelligence sharing with Iran," 20 June 2008.
[50] *Today's Zaman*, "Turkey Assures US over intelligence sharing with Iran," 20 June 2008.
[51] *Today's Zaman*, "Real-time intelligence involves fighter usage if necessary," 3 December 2007.
[52] *Today's Zaman*, "US cooperating on intelligence sharing," 9 October 2008.
[53] *Today's Zaman*, "Erdogan: US warm to Turkish request to base Predators in Turkey," 21 September 2011.
[54] *Today's Zaman*, "Washington not warm towards 24 hour intelligence sharing on PKK," 17 September 2012.
[55] *Reuters,* "NATO urges EU to boost defense ties with Turkey," 8 July 2008.

[56] *Today's Zaman*, "Turkey believes NATO members won't share intelligence with Israel," 6 October 2011.
[57] *World Bulletin*, "Israel kills Gaza activists on Turkish ship," 31 May 2010.
[58] *Today's Zaman*, "Israel to deliver two UAVs to Turkey in late November," 31 October 2008.
[59] *Reuters*, "Barak to promote Israeli spy satelites sale to Turkey," 12 February 2008.
[60] *Today's Zaman*, "Turkey vetoes Israel's latest NATO partnership bid, despite criticism," 23 April 2012.
[61] Ambassador Gabor Iklody, "NATO Assistant Secretary General for Emerging Security Challenges in New York. Briefing to the UN Counter-Terrorism Committee," 8 September 2011.
[62] Ambassador Gabor Iklody, "NATO Assistant Secretary General for Emerging Security Challenges in New York. Briefing to the UN Counter-Terrorism Committee," 8 September 2011.
[63] Partnership Action Plan Against Terrorism, 22 November 2002.
[64] *Xinhua*, "NATO Countries seek intelligence-sharing amid austerity," 17 March 2011.
[65] *The Guardian*, 20 December 2000. 'Intelligence Test' by Richard Norton-Taylor.
[66] *NPR*, September 24, 2001. "Analysis: Challenge of Sharing Intelligence With Other Countries."
[67] *Inside the Air Force*, Vol.15, No.2, 9 January 2004. "NATO Eyes Communication Architecture, But Now Links on Procedure."
[68] State Department Press Releases, "Rumsfeld Explains US Force Restructuring." 9 February 2004.
[69] *Agence France Press*, "Chirac and Schroeder call for increased cooperation against terrorism." 16 March 2004.
[70] State Department Press Release, "Text Of Declaration on Strategic Cooperation Between US and Republic of Poland." 20 August, 2008.
[71] *Today's Zaman*, "Belgian FM Reynders: We will act faster in intelligence sharing." 23 January 2013.
[72] *International Herald Tribune*, "France touts its role in NATO and ties to US security and intelligence efforts", 10 February 2005.

National Security of the Republic of Moldova in the Context of Actual Risks and Threats

Natalia ALBU[*]

Abstract

To ground the findings set forth in the given communication, it is important to use an analytical and conceptual approach to security, risk, and threatening notions, which allow point to us out the way in which security is to be learned, thought, and practiced. Analyzing from a gradual point of view, attention should be paid to the assessment of vulnerabilities, as they diminish the reaction capacity of the respective country to the existing or potential risks. In this context, the main internal vulnerabilities of the Republic of Moldova should be mentioned, which in current circumstances increase the role of external factors, representing the force which conditions security policies. For example, it should be mentioned the lack of control from constitutional authorities of the Republic of Moldova over the eastern part of the country. This vulnerability of the state induces risks and threats for regional security due to lack of control over production of military equipment and armament, which is under the control of the secessionist regime, creating conditions for the trans-border organized crime and illegal traffic of arms, drugs, and human beings.

Also, we talk here about the perspective of the small states with a weak potential to ensure their national security. Regardless of the situations mentioned in the respective communication, whenever we talk about the security of small and weak states, it goes without saying that currently the internal risks and dangers register a very high level, thus increasing the external ones.

Keywords: national security, risks, treats, weak and strong states, small and big states.

The way of the Republic of Moldova, as of most East-European countries, to an open society and a competitive economy, especially from its perspectives of democratization and market development has proven to be strongly dependent on the risks and security threats. Vulnerable to the external changes and unable to identify internally the priorities and necessary resources needed to modernize the public institutions, many states established after the disintegration of the USSR can be qualified as "weak states" and the insecurity and instability remained among the most important obstacles to the

[*] PhD in Political Science, Associate Professor, Military Academy of the Armed Forces "Alexandru cel Bun", Republic of Moldova

democratic stabilization of these states, which led to the persistence of extremely negative social effects for the population, for the state and civil society as a whole.

Thus, after becoming an independent state, the Republic of Moldova had to face a number of challenges to the national security and to overcome a range of risk factor. We are talking here about the threat for establishment and revival of imperial nature structures and positioning of the country outside the universal systems of collaboration and security. The existence of a regional environment which was not fully favorable for the Republic of Moldova was also generating problems, as it was marked by a zone of political instability and depressed economic circumstances. As a result, the Republic of Moldova was and still is located within the Russian Federation's interest space. Secondly, there still persisted the threat for maintaining and reactivating the ethno-separatist threats that could generate conflicts, meaning the conflict from the left side of the River Nistru. And thirdly, social internal pressures emerged due to the difficulties induced by the transition to the market economy. As compared to other states, Moldova's transition to the market economy was a rather long period characterized by crises and instability. As a result, the economic discrepancies between the Republic of Moldova and the countries of the Central Europe and CIS got deeper. We can also mention the mentality and the habits inherited from the soviet times. Fourthly, it highlights the dependence of a single sided power supply with energy agents that periodically marks not only the activities of the foreign policy of the Republic of Moldova but also the standard of living of the people by increasing the complaints, the poverty and uncertainty.

Additionally, the Republic of Moldova, just as other countries from the Eastern Europe is far from overcoming the world economic crisis in all its dimensions. The financial crisis and the economic recessions, which became more obvious in the majority of the world states, represents the result of assuming and promoting, consciously or unconsciously, some deficient management policies and practices which generate risks to national security.

To fundament these findings, it is important to tackle the analytical and conceptual approach to such notions as security, risk and threat – this would allow us pointing out the way in which security is learned, thought, and practiced. Today national security issues include all the vital interests of the country, society and citizens. The National Security Concept of the Republic of Moldova approaches national security in a larger framework, where it „represents the fundamental condition for the existence of the Moldovan state and the nation and is an object of government. Moldovan national security objectives are to ensure and defend the independence, sovereignty, territorial integrity, constitutional order, democratic development, internal security and consolidate the statehood of the Republic of Moldova. A special place in this regard lies with the defense and promotion of values, interests and objectives. National security is not only national security but also the security of society and citizens of Moldova, both in Moldova and beyond its borders”[1].

At the same time the actuality of the approached theme is determined by the need to define policies and identify some mechanisms that will prove to be able to contribute to strengthening national security of the Republic of Moldova, given the threats, risks and vulnerabilities that regularly occurs with different intensity. Practically the assertion expressed by D. Baldwin and E. Kolodziej has become axiomatic, stating that „security is a complex and controversial concept” both theoretical and methodological deficiencies but also an applicative character being determined by the author V. Juc , by a number of factors, such as:

1. growing interdependence between internal politics and foreign policy in a globalized world where is reduced the strict delimitation between national and international

2. decentralization and expansion of the number of international actors, the gradual transformation of international relations from political strict or, in other words, interstate in transnational including and other agents;

3. stratification of security, became a complex category that includes various levels, from the individual up to global, each including special values and interests. These differences derived from the lack of a common base have not favored the agreement according to the definition of security that would include strategies and

mechanisms „designed as nonviolent and used by actors" directed towards minimizing the threats, the counteraction of risks and the reduction of the intensity of vulnerabilities, surpassing the motivations to cause and supply the insecurity both at the agents level as at the systematic one[2].

The variety of approaches of security allows us to ascertain that the concepts of risk and threat are often found in the definition of national security. A. Wolfers supports the idea that „in an objective sense, the security measures the lack of threats that presses on the acquired values; in the subjective sense, they designate the absence of fear that these values will be attacked"[3]. The author Barry Buzan in his famous work „Nations, States and Fear" broadens significantly the field of analysis and application of the concept of security, supporting the idea that „in case of security, the discussion consists in minimizing the threats".[4] It is important to mention the fact that this author addresses the issues of interdependence between the internal and external threats of national security, which is currently in the context of the process of globalization. In this context we highlight also the *globalist paradigm of security*, for which the "security" concept is very close in meaning with "stability". Internal stability is defined as integrity of the political system; promotion of democratic norms, including the regulate rotation of governing elites; absence of ethnic and social conflicts; a healthy economy which functions normally[5].

Beyond these definitions, we find that all the risks, dangers and threats concerning the national security of a state, recorded up to this stage, are too broad. The Republic of Moldova faces threats common to the entire international community: the rise of terrorism, illegal arms trade, drug trafficking and illegal migration, international crises and unsolved conflicts, not least the organized crime etc. Respectively, the purpose of all security policy must ensure safety at four levels: individual (citizens), collective (associations of interest), national (state) and international (external environment). This supposes a continuous adjustment of the national security system at external and internal environment to meet new security challenges and security issues at all five dimensions: political, military, economic, environmental and social. Thus, the threats and risks assessment which is exerted or may exercise over the security of a state can not be produced by a pattern, but takes complex forms.

When analyzing the threats which are manifested currently and/or in the near future, directly or indirectly, we can say that they are internal, external or combined. These threats have become “chronic” for the Republic of Moldova as a consequence of the state’s internal vulnerability and lack of well-articulated political institutions in the national context. Nevertheless, the external threats remain to be a concern, as security or lack of security are defined in correlation with external and internal vulnerability which endangers or undermines the capacity to ensure the national security of a state.

In this context, the author Mohamed Ayoob, when analyzing security from the perspective of the third world countries, supports the idea that although the internal crisis of a state may be considered to be a potential factor for destabilizing the security of the respective state, it will depend on the space and temporal context so as to consider a specific situation to be a threat or not[6]. For instance, the problem of disappearance of a strategic resource, such as petrol of water, may be vital for a country and may be considered to be a security problem, while in another state, this problem is not part of the threats induced to the national security. First of all it concerns a threat to security in the case of a developing country. On the other hand, the conflict regarding the strategic resources can be transformed into a threat to the economic security of a state. Long-term, the security of a state, including the Republic of Moldova, depends on its economic capabilities that allow it to protect the interests of the country. In the specialized literature, sometimes, when we talk about risks and threats to the national security, reference is made to “weak and strong states”[7]or “small and big states”[8]. Barry Buzan considers that “the distinction between weak and strong states is essential for any analysis of national security”[9]. Weak and strong states – the level of social-political cohesion is taken into consideration; weak and strong powers – refer to the economic and military capacity. Such weak powers as Austria, Holland, and Norway are all strong states. While such important powers as Brazil, Pakistan, and Indonesia are considered to be weak states. The super-power from old times, USSR and today China are classified as weak states because of the social-political indicators.

In general, the weak states are considered to be the source of insecurity. *First of all,* there are weak states as a result of a dependency on a bigger power (for instance, the situation of the states from the Latin America, which are dependent on the United States or the CIS member states – which are dependent of the Russian Federation). *Secondly,* there are weak states, especially from the third world and the former USSR, within which the fundamental statehood elements (population, identity, territory, and institutional structure) are insufficiently or precariously defined. *Thirdly*, there are weak states among the countries which although have achieved a form of internal cohesion (usually through authoritarian political regimes) manifest themselves on the international plan as powerful sources of instability and insecurity (Northern Korea, Libya, Cuba). A common feature for all the weak states from any of the above-mentioned categories is the high level of internal risks, which anytime may transform into threats for the government, because the "weak states either do not have or did not succeed to come to a political and societal consensus of enough stability so as to eliminate the large-scale use of the force, as a major element and continuity in the nation's political life".[10]

When the state is strong, national security refers, especially, to the protection from external interferences, as it is considered that within the state the institutions operate in optimal way, the territory is well defined, and the mechanisms of power transfer do not endanger political stability. When the state is weak, security assurance refers to both: external and internal threats.

Actually, the analysis of risks and threats for the national security from the perspective of the "weak or powerful state" is part of a larger framework of discussions and namely the security of the "small or big state". The adepts of the small states' classification through the power perspective are the representatives of the political realism, for which the power is "the capacity to influence the decisions of other states". Power is inherently associated with possession of human, natural, military rights, territory, economic potential, political stability, national cohesion, etc. If previously the small state was delimitated only by geographical criteria (territory, population, presence of natural resources, etc.), today the technological development, educational system, and economic growth are the most important indicators of a state's power, although the military factor also remains to be a very important factor[11]. The comparison between Sweden and Japan is relevant for this purpose. Although both countries differ considerably from territory point of view (Sweden - 450.000 km², Japan - 372.200 km²), Japan is unanimously recognized as a big power, while Sweden is considered to be a small state. At the same time, both states have very big economic potential and both of them are able to ensure their own security, although through different approaches. Hence, it is the geographical localization and not the geographical size that counts for the security of small state. This comparison also points out another important aspect, and namely the fact that a small state is not mandatory also a weak state, although in reality, the majority of small states, including the Republic of Moldova are weak and very weak states[12].

Thus, when analyzing the nature of risks and threats to national security, it is important to pay attention also to the nature of the state – big or small and strong or weak. For us, the most relevant opinions are the ones that tend to dominate the thinking about small states' security. First of all, the perspective of small states is analyzed from their survival point of view, which depends on what this state can do to ensure its security. From this point of view, it is important to pay attention to the state's internal perspective, where the actions of the small states may have considerable impact on their final fate. The long-term survival depends on the state's diplomacy quality, on finding correct policies, the best-thought direction and the "wisest" approach[13]. Thus, the conclusion may be drawn, that although the Republic of Moldova is a small state, this is not a justification for the external implications for the national security. In this analysis framework, internal risks' and threats' mitigation is the most important action.

Secondly, there is an opinion that the security of the small state is determined by external factors. In this respect, the policies of the big powers are considered to be determinant for the destiny of the small states, and previously we called this fact as *dependency*. At the same time, it is undeniable the fact of exercise of pressure from the great powers over the states situated in the geopolitical/ geostrategic interest zone, which are at the boundaries of these entities in the "buffer zone".[14] The evolution of the *geopolitical situation of the Republic of Moldova* influences the increase or the decrease of the risks to the national security, although in the globalization process context, *geopolitics* is frequently condemned to lack of actuality, when globalism should go beyond the geopolitical pressures[15]. Nevertheless, we consider that the influence of the geopolitical space on the Republic of Moldova's security is a complex and important problem as for any other state. For Moldova, the process of choosing the geopolitical vector is very difficult in all the areas, but the historical development path of Moldova as European state is related to European integration. In Europe's new architecture, the place of the Republic of Moldova is determined by its location, as it is in the confluence of three political-geographical regions: Central Europe, South-Eastern Europe, and Eastern Europe. After the collapse of the Soviet Union, Moldova did not interrupt its relations with the former soviet republics due to economic reasons, so as to keep the external sale markets and to ensure itself energy resources and raw material. Hence, choosing the vector for Moldova's integration with European Union or Russia depends on the geopolitical interests and orientations of these actors, as well as on the Republic of Moldova's dependency on external energy resources.

The Republic of Moldova and Georgia initiated separately the Association Agreement with European Union, the 29th November 2013, at Vilnius, shortly before the beginning of Eastern Partnership Summit[16]. After signing the historic agreement with EU, the Moldovan Prime Minister Iurie Leanca said: "We are living a historic moment, signing an agreement with unprecedented ambitions which means trust, openness, and cooperation"[17]. The importance of the moment, as the need for a rapid and a well thought sector policies in Chisinau, Brussels and Washington, which makes feasible the security and the welfare of the region and the European Continent. Beyond the discontentment related to the separation of the Balkan region, which has the prospect of accession to European Union, for the Republic of Moldova "the Eastern packet" constituted a regional coverage in an attempt of detachment from post-Soviet history. However, the approach to the problem related to the Republic of Moldova's integration into the European Union implies finding answers to a number of questions. Nevertheless attention should be paid to the fact that such problems as internal political stability, energetic and commercial policies, the Transnistrian problem became more dependent on Russia's and Ukraine's behavior.

At the same time, the Republic of Moldova does not develop any prospects for integration into the Euro-Atlantic structures in order to ensure the national security, although the mechanism, multiple treaties and agreements signed within the CIS are not effective to the regional cooperation in the field of security. But our country's integration into European structures depends on the role that is assigned to Europe in the context of strengthening the European security. Recently it was important the phrase that "The Republic of Moldova is an important state in the context of security and stability in Europe" or it is "a hotbed of regional instability". During the last years, the situation in Transnistria, controlled by pro-Russian separatist forces, became a challenge to security interests and democratic values of the extended Euro-Atlantic community. The fact of Romania's accession, neighbor state, as a full member of NATO, as well as Ukraine's previous statements on its accession to NATO, seems to have changed the format of regional geopolitics. We cannot overlook the specific of political and military security arising from the geographical location of Ukraine. As a regional power, Ukraine may contribute to changes in the European security system, in case of a possible conflict between Ukraine and Russia. To the same extent, the possible regional integration of Ukraine and Russia could lead to a destabilization of the situation on the European continent, and the potential of this state may, to some extent, to change the power balance that was created between NATO and Russia. Moreover, Ukraine has role as a regional economic actor on whose territory the energetic ways towards Europe are located.

In substantiation of the above mentioned, we can bring as an example the *Vilnius Summit of the Eastern Partnership* in Autumn 2013. Representatives of the Slovak Foreign Policy Association, after analyzing the way they honored the undertaken commitments of Eastern Partnership countries to European Union, formulated four possible scenarios before the summit. In this context, we draw your attention to the second scenario that is a positive one only for the Republic of Moldova and Georgia, the countries which will initiate the Association Agreement with the European Union. However Ukraine will not sign this document at Vilnius, as a result, the Russian influence in this country becomes greater. Although it relied on the fact that Ukraine will sign[18] and the Republic of Moldova will initiate, however Ukraine succumbed to Russian pressure and announced a few days before the signing of the Association Agreement with the European Union that suspends any negotiation[19]. The fact that Ukraine means, at the moment, the Eastern partnership "first violin" is proven by the interest for "Euromaidan" and the Ukrainian domestic political situation after Vilnius[20].

So, Ukraine's role in regional security is important. The geostrategic orientation of Ukraine is not constant, and the events which occurred in Ukraine tell us that we cannot rely on Ukraine's support when integrating in EU or joining NATO, or even when settling the Transnistrian conflict. The problems related to the Republic of Moldova's properties on Ukraine's territory, borders' delimitation, the Giurgiulest terminal, and Palanca segment, but moreover the problems related to the impediments for transiting Moldovan goods through Ukraine's territory when exporting them to the SIC space have shown that Ukraine is not a safe partner. Here we can mention the material presented by Iulian Chifu, *Security Options of the Republic of Moldova*[21], where *the Costs of the current security situation of the country* are assessed. Although the expert tackles objectively the situation of the Republic of Moldova as vulnerability for the EU, NATO and its neighbors, including for Ukraine, however the internal development from Ukraine after Vilnius presents a threat to regional actors' security, especially for the Republic of Moldova, which can even lead to major risk factors in "Transnistria".

But whatever the situations previewed above, when talking about the security of small and weak states, it is clear that at the current stage the risks and the dangers of internal nature remain at a high level, which enhances the external one. In this context, it highlights the lack of progress in the Transnistrian conflict settlement. Transnistrian conflict imposed externally to the Republic of Moldova by invoking imaginary dangers marked profoundly its political history and narrowed substantially the field of diplomatic maneuvering. In the concept of national security of the Republic of Moldova we mean the main threats to national security of the country, where the main threat is the conflict of the left bank of River Nistru[22]. Certainly, the Republic of Moldova cannot become a truly viable state as long as there is the Transnistrian issue, the reintegration of opportunities supposing favorable international circumstances, but which should be framed in a broader context, accompanied and reinforced by increased efforts and concrete actions with internal character[23].

Unauthorized stationing of Russian military forces in the districts on the left bank of River Nistru and the their withdrawal opportunity conditioned also the unilateral decreeing of the state initial of demilitarized zone, and later permanent neutrality, conditions that are incompatible with “the deployment of troops of other states on its territory” and represent a component of national security. This constitutional provision is developed and concretized in the concept of national security of the Republic of Moldova.

However, self-proclaimed permanent neutrality, according to N. Osmochescu, “remains a fiction”[24][25]. The fragility of neutrality status is largely determined by the fact that the unilateral declaration of such status is insufficient for its viability. Deprived of an effective guarantee from the major powers or an international recognition (supportive), the neutral state may rely, exclusively, only on its own forces in order to ensure its security and rejection of a possible aggression.

From the perspective of public international law, N. Osmochescu emphasizes that the effectiveness of self-proclaimed neutrality is depreciated by the fact that was not object of recognition and guaranteed by international agreements or other arrangements, as are the cases of Switzerland, Austria, Malta and Turkmenistan. Unfortunately, we find that the unilateral declaration of the permanent neutrality status by the Republic of Moldova, has not been followed by other actions in this regard, it has not led to the respect and the withdrawal of Russian military troops.

Starting from the fact that the respect and the recognition of permanent neutrality status is based primarily on the credibility of this state and namely on the efficiency of the internal forces of the state in providing a credible defense, is absolutely illogical to hope that the Republic of Moldova will be recognized as a neutral state exclusively on foreign policy actions, as actually provides the national security concept [26].Thus, permanent neutrality declared unilaterally and maintained by its own will did not contribute to capitalizing on strategic objectives pursued, being defied and depreciated by the presence of foreign military forces on its territory, even if temporary is under the control of the secessionist authorities.

Returning to the Transnistrian conflict is indisputable the fact that the districts from the left bank of River Nistru can be neither abandoned nor exchanged or transferred, the unification of the country being awarded to the primacy in value terms, or this noble desideratum should not be a goal to be solved at any price and to the detriment of national interests: maintaining the dialogue and seeking strengthening solutions to build confidence and sustainable regulatory, the conflict can stay longer “frozen” and the final defusing be transferred to another generation of political leaders, as occurs in Cyprus and especially of Korea. Q. Wright identified four ways of regulating the conflict – the parties fall agrees, a part impose solutions to another protagonist, a third force propose/ impose solutions, the conflict loses its timeliness and resolves itself[27].

The recent international practice demonstrates that unilateral recognition of secessionist regimes in the former Soviet Union and former Yugoslavia by some or more great powers themselves do not present effective solutions and nothing changes in political and legal statutes, sustainable regulatory, in our opinion, assuming the application of the first ways described by Q. Wright. It should be noted, however, that the conceptual foundation of management of “frozen conflicts” remains not only a political-legal issue but a theoretical-methodological one, since the ancient settlement mechanisms such as condominiums or partnering with the opponent are no more applicable.

Taking as basis the German model of reunification of the country, we believe that the issue of East districts can be solved more easily and sustainably in conditions of positive perception (attractive) of the Republic of Moldova at the daily level by the inhabitants of the left bank, especially when we are talking about standard of living and free movement in the European Union. It is important that the integration of the country is not an impediment to the process of European integration, and the Republic of Moldova should take advantage of openings from the sides of European structures, which show an increasing attention to the processes that occur both in finding solutions to the conflict in the left bank as well as in general course promoting towards democracy[28].

In conclusion we mention the idea that improving these and other threats, risks and vulnerabilities urgently require the identification of some alternatives designed to help ensure and strengthen national security of the Republic of Moldova, including:

- Proclaimed status by permanent neutrality did not contribute to the achievement of the security objectives, as a result it would be the case of to strengthen ties with the North Atlantic Alliance, which will bring advantages, including the acceleration of European integration, even if some tensions and controversies will soon appear.

- Identifying alternative sources of supply of energy agents by participating in European Union projects (implementation of the Energy Community Treaty) and their contracting countries of Transcaucasia and Middle East, using the maximum capacity of Giurgiulesti and in perspective the possibility of importing methane from other sources such as gas pipeline Ungheni-Iasi. In the same context it includes harnessing alternative local sources.

- Diversification of markets for goods and products by signing an asymmetric trade agreement with the European Union, requesting the extension of the list of titles in the account of food products etc.

Therefore, the correct identification of risks and threats to national security of the Republic of Moldova contributes to structure the actions necessary to strengthen the national security of the country, starting from the idea that no country is able to deal with today's complex problems on its own. In the same time, the national security options of the country require the adoption of a solid decision, consistent and valid of security, which to be assumed, sustainable and supported by the population.

References

[1] *Concepţia securităţii naţionale a Republicii Moldova*. Parlamentul Republicii Moldova, Lege nr. 112 din 22.05.2008, in: *Monitorul Oficial al Republicii Moldova*, nr. 97-98 din 03.06.2008.

[2] Victor Juc., „Oportunităţi şi alternative de consolidare a securităţii naţionale a Republicii Moldova", *Revista de filosofie, sociologie şi ştiinţe politice*, vol. 154, no 3, Institutul Integrare Europeană şi Ştiinţe Politice al Academiei de Ştiinţe a Moldovei, 2010, p. 11.

[3] Arnold Wolfers. *Discord and Collaboration: Essays on International Politics*. (Baltimor: Johns Hopkins University Press, 1965), p. 159.

[4] Barry Buzan. *Popoarele, state şi teamă*. (Chişinău: Editura Cartier, 2000), pp. 18-19.

[5] Вячеслав Сенчагов. *Экономическая безопасность, геополитика, глобализация, самосохранение и развитие*. (Москва: Финстатинформ, 2002), p. 42.

[6] Ghica L. A., Zulean M. *Politica de securitate naţională*, (Iaşi: Polirom, 2007), p. 83.

[7] A se vedea: Barry Buzan. *op. cit.*; Ionel Nicu Sava. *Studii de securitate (*Bucureşti: Centrul Roman de Studii Regionale, 2005).

[8] Valeriu Prohniţchi, Securitatea economică a unui stat mic. Note de reper pentru Republica Moldova, *i*n: *Securitatea şi apărarea naţională a Republicii Moldova*. (Chişinău: Editura ARC, 2002), pp. 148-195. Toma A. *Globalizarea: provocări, riscuri şi pericole*. (Chişinău, 2005).

[9] Barry Buzan. *op. cit.*, p. 97.

[10] Buzan B. *op. cit.*, p. 99.

[11] Valeriu Prohniţchi. „Securitatea economică a unui stat mic. Note de reper pentru Republica Moldova", în: *Securitatea şi apărarea naţională a Republicii Moldova*. (Chişinău: Editura ARC, 2002), pp. 7-9.

[12] Jon Hindmarsh. „How do we define small states and islands? A critical analysis of alternative conceptualizations", in: *Convergence*, Vol. 29, no. 2, 1996.

[13] Andrei Toma. *Globalizarea: provocări, riscuri şi pericole.* (Chişinău, 2005), p. 89.

[14] Victor Juc, Ivan Rusandu, Veaceslav Ungureanu. „Consolidarea securităţii politice a Republicii Moldova: aspecte geopolitice", in: *Moldoscopie*, nr. 2(XLIX), 2010, p. 154.

[15] Eugen Bădălan. *Securitatea Romaniei: actualitate şi perspective.* (Bucureşti: Editura Militară, 2001); „Bilan de trente ans de globalisation. Commentaire". În: *Le Matin*, nr. 20, 22 septembre, 1999.

[16] NOTE: Eastern Partnership in the formula of political association and European economic integration focused above all Ukraine, then the Republic of Moldova and other post-Soviet states.

[17] *Summitul de la Vilnius ziua II: Republica Moldova parafează Acordul de Asociere cu UE. Vedeta geopolitică, Ucraina, ramâne mai departe cu Rusia/ Premierul Iurie Leancă: Moldova, astăzi am asigurat drumul nostru spre Uniunea Europeană*, accessed 12 December 2013 at http://m.hotnews.ro/stire/16095310

[18] NOTE: Ukraine initialed the Association Agreement in 2012.

[19] Alexander Duleba, András Rácz, Věra Řiháčková, Rafał Sadowski. *Visegrad 4 the Eastern Partnership: Towards the Vilnius Summit.* (Bratislava: Research Center of the Slovak Foreign Policy Association, 2013), p. 30.

[20] Eduard Ţugui. „De la Vilnius la Riga: Republica Moldova şi dinamica Parteneriatului Estic", in: *Buletinul de Politică Externă*, nr. 73, decembrie 2013, p. 2.

[21] Iulian Chifu. *Opţiunile de securitate ale Republicii Moldova,* pp. 34-35, accessed 7 September 2013, http://www.cpc-ew.ro/pdfs/carte_202.pdf

[22] *Concepţia securităţii naţionale a Republicii Moldova.* Parlamentul Republicii Moldova, Lege nr. 112 din 22.05.2008. În: *Monitorul Oficial al Republicii Moldova*, nr. 97-98 din 03.06.2008.

[23] Victor Juc. „Oportunităţi şi alternative de consolidare a securităţii naţionale a Republicii Moldova", in: *Revista de filosofie, sociologie şi ştiinţe politice*, vol. 154, no. 3, Institutul Integrare Europeană şi Ştiinţe Politice al Academiei de Ştiinţe a Moldovei, 2010, p. 13.

[24] Nicolae Osmochescu. „Neutralitatea permanentă a Republicii Moldova în contextul relaţiilor internaţionale contemporane", in: *Academia de Administrare Publică – 15 ani de modernizare a serviciului public din Republica Moldova*. Vol. 2.

Materialele conferinţei internaţionale ştiinţifico-practice. Chişinău: AAP, 2008, pp. 182–183.

[25] *Ibidem*.

[26] Iurie Pîntea, David Hellz, Polina Panainte. *Perspectivele cooperării Republicii Moldova în cadrul Politicii de Securitate şi Apărare Comună.* (Chişinău: Casa Editorial-Poligrafică „Bons Offices", 2011), p. 31.

[27] *Социальный конфликт: современные исследования.* Реферативный сборник. Москва: ИНИОН, 1991, pp.82–83.

[28] Victor Juc. *Oportunităţi şi alternative de consolidare a securităţii naţionale a Republicii Moldova*, in: *Revista de filosofie, sociologie şi ştiinţe politice*, nr. 3 (154), 2010. Institutul Integrare Europeană şi Ştiinţe Politice al Academiei de Ştiinţe a Moldovei, 2010, p. 18.

Theoretical and National Aspects of National and International Provisions in Assuring Aeronautic Security Field

Vitalie SÎLI[*]

Terrorism, being a socially dangerous phenomenon and having major negative impact on important social values protected by the Criminal Law, tends to acquire new forms of exteriorization which might draw a growing response and contribute to assuring some real possibilities for promoting terrorist ideology. In this context, terrorist followers permanently try to use the advantages of the technological progress for their purposes. Unfortunately, in the majority of cases, law enforcement institutions and special services have to merely state new manifestations of terrorists' ingenuity, exteriorized through the diversification of forms and methods used for achieving their aims. The so-called aviation-related terrorism has undergone the same evolution.

The sweeping development of technologies, which was registered especially in the last century, alongside with the enormous possibilities it offers in the everyday life, has also led to an increasing number of threats that spring from using facilities, machinery and equipment for terrorist purposes. Conquering the space, humanity has solved a major problem- saving time by transporting passengers and cargoes in space. But from another perspective, the space has started to be used in military purposes, letting States that had the control thereof, which literally had a much larger number of modern aircraft, to ensure the victory even in the most complicated military confrontations.

So in time, the diversification and extension of the airspace use possibilities took place and aircrafts became an essential element of modern human civilization. However, the multiple commodities that aircrafts offer have been reduced by the dangers they accompany.

[*] Intelligence expert, Republic of Moldova

These dangers increased significantly when airplanes in quite a short period of time have become terrorist targets, initially being used as leverage for promoting criminal concepts and subsequently as means for committing terrorist acts.

Aircraft seizures took place in Moldova as well. In the history of the Republic of Moldova, as well as in the history of the former Soviet Union, one of the first attempts of hijacking a plane An-2, was made on September 29th, 1964. The plane had a flight from Chişinău with stopovers in Ciadir-Lunga, Bolgrad and Izmail, ultimately planning to land back in Chişinău.

In Ciadîr-Lunga, two persons with records of convictions, immediately after the takeoff, entered the cockpit and, threatening the pilot with a gun, ordered him to direct the plane towards Turkey. The pilots managed to redirect the plane to Chişinău airport. At the landing, the hijackers, having noticed in the side window the city buildings, realized that their criminal intentions were unsuccessful. They injured heavily the pilots with knives and fire arms. Yet, the pilots managed to land the aircraft in the vineyard near the city.

The correct actions and heroism of the pilots helped to prevent the offense. Later, as a result of law activities carried out by law enforcement agencies and special service, one of the hijackers was detained, and the other, offering resistance and shooting two police officers, was killed in the course of his detention.

At the international level, the terrorists' actions urged the adoption of international conventions in this field.

Thus, in 1970 from the 6th of September till the 11th of September, the terrorists from the group “Black September”, together with National Palestine Liberation Front's adherents, hijacked 5 aircrafts with passengers on board. These aircrafts were placed by the terrorists in a desert. After the hijackers' claims were met, the passengers were freed and the aircrafts, on Yasir Arafat's order, were destroyed. This was the reason for stimulating the international community and adopting till the end of the year a Convention on the aircraft seizure prevention.

In general, particular methods were used regarding aircraft which have become the target for the terrorist attacks. They can be grouped in the following categories:

- aircraft hijacking;
- organizing explosions aimed at damaging or destroying the aircraft or people's murder;
- armed aircraft attack aimed at passengers' murder or hostage seizure.

Assuring aeronautic security should be given special attention because of its vulnerability in front of critical situations which can appear in the process of its use and extremely negative effects which can exteriorize by destruction or disposal of the aircraft and murder of the passengers and the crew thereof. A particular aspect related to the air transport consists in the international character of the aeronautic security crimes. Thus, it should be mentioned that in situations related to air transport, the state to which the aircraft belongs, the state on whose territory it has landed, the state whose passengers are on board, etc., are involved.

The practical realization of aeronautic security becomes essentially complicated because of the big number of passengers, big number of aircrafts implicated in air traffic, diversification of companies which offer services in this domain, as well as airports that are destined to offer possibilities of flight, landing, navigation and maintenance of aircrafts. So, according to some facts, in the air transport network are implicated more than 6800 airports, services being accorded by more than 3000 air companies, which transport more than two million passengers every day.

There is no doubt that in the case of a big number of passengers and a big number of subjects who have charge of this kind of activity, the problem of assuring security rises at a new qualitative level, having the need of major efforts and multilateral investments.

Due to the technical evolution there is a constant possibility of appearance of some new types of terrorism. In this context, we establish that it scientific is possible to commit new actions by the terrorists in the direction of using in criminal aims, of new technical performances. In this situation undercover men of organs of protection of legal regulations, the leaders and the specialists of enterprises, that could become object of acts of terrorism, should manifest ingenuity not smaller than terrorists, to simulate the possible variants of criminal actions and to elaborate preventive security measures for defending the potential objects from acts of terrorism.

Frequently, especially in case of political motivated actions, as objectives of acts of terrorism could appear citizens that have nothing in common with the administrative organs of state, with political or social activitiesp.

One of contemporaneous terrorism tendency consists in expansion not just of objective spectrum upon which terrorists attempt, but also of the purpose of their use. Let's take for instance an aircraft – a simple charter plane. Until recently there were 3 basic reasons for terrorist attacks on this type of transport, namely:

1. The aircraft could be destroyed by terrorists as being a valuable material object in order to demonstrate the gravity of acts and the potential of the terroristic organization. A stronger resonance, so eagerly desired by terrorists, occurs in case when plane with passengers on board is destroyed.

2. The plane's board is considered by terrorists a very convenient place for taking the passengers as hostages. At the same time the plane board is easily controlled even by a small group of terrorists. The big density of people and the rising risk of damaging innocent people during the antiterrorist operation lead to the situation when law enforcement agencies rarely authorize the storming of the captured plain.

3. Terrorists, using plane board as a temporary prison for hostages, use at the same time the aircraft as means of transport with quick mobility, a fact which permits the quick change of location and creates impediments for special antiterrorist units in taking the offensive.

However, from September 11, 2001 terrorists have ascribed to aircrafts another dangerous function. Thus, plains with full tanks can be changed into air bombs with huge power and high accuracy due to kamikaze terrorists' precise aircraft positioning in relation to the target.

On the board of the 4 stolen aircrafts on September 11, 2001 that struck the buildings of World Trade Center, Pentagon and another aircraft that has fallen at the distance of 120 km from Pittsburg, there were 19 terrorists – the authors of skyjacking, and

247 passengers, that did not have any chance to be rescued. In addition, under the ruins of Pentagon and the buildings of World Trade Center died about 4000 people.

Also, it has to be mentioned that the attacks expenses varied from 250.000 to 500.000 US dollars, and direct losses were estimated to 30 billion US dollars. The total loss estimation, only in New York, is calculated to be 83.000.000 US dollars (according to prices in 2001). Thus, the ratio between terrorists' expenses and total losses caused to the USA is 1 to 60.000. It is extremely difficult to estimate total losses (only several sums: insurance expenses - 40-50 billion US dollars, New York capital losses – 30 billion US dollars, municipal cleaning costs – 14 billion US dollars, airlines losses costs – 15 billion US dollars, expenses for increasing security measures – 10 billion US dollars, etc).

The evolution of international legislation in the field was determined by these events and by major negative impact upon the airports and civil aviation security segment.

Thereby, in order to ensure legal regulation of issues concerning this field, there has been adopted a series of International Conventions, for example:

1. Convention on Offences and Other Certain Acts Committed on Board Aircraft, signed on 14.09.1963, in Tokyo;
2. Convention for the Suppression of Unlawful Seizure of Aircraft, signed on 16.12.1970, in Hague;
3. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed in Montreal on 23.09.1971;
4. Convention on the Suppression of Unlawful Acts relating to International Civil Aviation, signed in Beijing on 10.09.2010.

Afterwards, in order to adjust, complete and modify the mentioned Conventions in accordance with the objective reality, there were adopted: The Protocol Supplementary to the Convention for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, concluded in Montreal, on 24.02.1988 and the Protocol Supplementing the Convention for the Suppression of Unlawful Seizure of Aircraft, concluded in Beijing on 10.09.2010.

Furthermore, there were adopted some international acts with the purpose of indirectly assuring the civil aviation security. As an example, it can be mentioned the Convention on the Marking of Plastic Explosives for the Purpose of Detection, adopted in Montreal, on 01.03.1991.

As a basis for the mentioned conventions adoption have served illicit actions, directed against the safety of civil aviation, and skyjacking, which endanger the security of people and goods, seriously obstruct the use of air services and undermine people's trust in civil aviation security.

The above mentioned conventions regulate the fields specialized in assuring civil aviation and airport security. In order to improve the practical performance of legal provisions, within the conventions' framework are included some general notions that are to be implemented in national legislation. Thus, in the text of conventions, which are object of investigation, are included notions such as: aircraft in flight, aircraft on duty, jurisdictional competence of states, rights and obligations of an aircraft commander, rights and obligations of states, rights of the person arrested for perpetrating or intention to perpetrate a crime on the board of an aircraft, the procedures and methods of solving state differences.

The main convention aspects imply the separation of competences and measures that have to be undertaken depending on the fact if the relationship is to be established between contracting countries, parties to the conventions, and between contracting countries, on one side, and no-contracting countries, on the other side (ltr. a, paragraph 1, article 8 of the Convention on Offences and Other Certain Acts). It is also mentioned the need to delimitate civil aircrafts and those used in military, customs or police, which do not fall under these regulations.

Practical significance for preventing and fighting against crimes in the civil aviation segment is attached to the right perception of important concepts in this context.

Thus, in the context of mentioned conventions, *an aircraft* is considered to be *in flight* when the embarkation is finished and all exterior doors are closed, until the moment when at least one of these doors is opened for debarkation. In case of emergency landing, the flight is considered continuing until competent authorities accept the aircraft, as well as people and material goods on the board.

Initially, in par. 1, art 1. of the Convention on Offences and Other Certain Acts Committed on Board Aircraft of 14.09.1963, in addition to the mentioned definition, was stipulated that an aircraft is considered in flight since the moment when the motive force is used in order to take off, until the landing. However, in later adopted conventions this definition is omitted. We consider that this is due to the incapacity of systematizing all dangerous actions that threaten civil aviation security in this provision. In such context, in order to ensure the possibility of preventing and efficiently fighting against crimes committed in the field the mentioned conventions work, the idea of expanding the definition concerning an aircraft in flight was supported. Also, the fact of accepting the broad sense of the definition concerning an aircraft in flight permits a better determination of jurisdiction and contributes to avoiding conflicts of interest among states.

Another notion that appears in conventions is *aircraft on duty*. Thus, according to ltr. b, par. 2 of the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 23.09.1971, *an aircraft on duty* is considered to be since the moment the crew begins to prepare the aircraft for the flight, until expires the term of 24 hours from any landing. As we see, the time of duty covers anyway the whole time the aircraft spends in flight.

A special attention is paid to the establishment of competences in case the committed crimes fall under mentioned conventions.

Thus, according to art. 3 of the Convention on Offences and Other Certain Acts Committed on Board Aircraft, the state where the aircraft is matriculated has the right to carry out jurisdiction upon crimes and acts committed on aircraft board. Besides, each contracting state will take measures in order to establish its competence of matriculate state, having the goal to carry out jurisdiction upon committed crimes on board of the aircraft notified in its matriculation register.

Simultaneously, as it is resulting from article 4 of the Convention for the Suppression of Unlawful Seizure of Aircraft, any contracting state will take the necessary measures in order to establish its jurisdictional competence regarding the crime and also any act of violence against the passengers or against the crew and committed by the suspect author of crime in direct liaison with it, in the following cases:

a) if the crime is perpetrated at the board of an aircraft registered in this state;

b) if the airplane at the board of which the crime has been committed is landing on its territory and the suspect author of crime is still on board;

c) if the crime is committed on the board of an aircraft without crew, rented to a person who's the main office is on the territory of this state, or in its missing, has a permanent residence in this one.

In the same meaning, any contracted state will also take the necessary measures in order to establish its jurisdictional competence regarding the crime, in case the crime suspect is on its territory and when this state is not extraditing him to one of the competent states to investigate and judge the respective case.

If the contracting state will assess that the circumstances will justify these actions, it will ensure the detention or any other measures will be taken in order to assure the presence of the person considered to be the author of an illegal act stipulated in the international conventions, and also any other person who will be transferred to the respective state. The detention and the other measures must be according to the law of that state, and can be maintained only for the necessary period in order to begin the criminal investigation or another extraordinary procedure. Any detained person must be provided with all the possibilities for contacting immediately the nearest official representative of the state whose nationality this person has.

In case when a state accepts a person on detention, this one will inform immediately about this detention and also about the circumstances which justify it:

1. the registering state of the aircraft;

2. the state whose nationality the person on detention has;
3. any other interested state.

If the person who has been dropped off because of committing or was on the way to commit an illicit act on the board of the aircraft, cannot or does not want to continue the travel, the state on which territory the landing took place, if refuses to accept this person on its territory and if this person does not have the nationality of the respective state or does not have permanent residence on its territory, can deport this person to the state whose nationality this one has or where his permanent residence is, or to the state from which territory the person started its air travel.

From the standpoint of extradition, international statutory acts offer ample possibilities for ensuring the practical implementation of the principle aut dedere aut judiciare (extradite or judge). Thus, the extradition between the contractor states can take place on the basis of an agreement of extradition concluded between them. This agreement has to govern the crime for the perpetration of which the person will be extradited, if such an agreement exists. In case a contractor state that subordinates the extradition to the existence of an agreement is notified by a request of extradition from the part of another contractor state with which it is not bound by an agreement of extradition, it has the latitude to consider the conventions in the field as being a legal basis for extradition regarding the specific crime. Also, between the contractor states, the crime is considered as to extradition being committed both at the site of its perpetration and on the territory of states, which have to establish their competences. An important provision concerning the extradition, is stipulated in article 16 of the Convention on Offences and certain Other Acts Committed on Board of Aircraft, according to which offences committed on board of aircrafts registered in one of contractor states are considered, with a view of an extradition, being committed both at the site of their perpetration and on the territory of the state registering the airplane.

For the purpose of ensuring an efficient and prompt reaction regarding persons who committed or are suspected to have committed a crime that is related to the framework of convention which have as objective ensuring aeronautic civil security, the operational method is mentioned in case of situations that follow under the scope of activity of these conventions. Thus, the contractor states will provide each other with the largest possible judicial assistance in any criminal proceedings regarding the offences stipulated in the text of conventions [2, articles 10; 3, article11]. In all cases the law of the state to which the request is addressed is applied for the fulfillment of an assistance request.

In addition, the contractor states must report as soon as possible to the Council of the International Civil Aviation Organization, according to the provisions of their national legislation, any kind of information they have, regarding:

a) circumstances of offence perpetration;

b) measures undertaken in order to prevent offences, ensuring the possibility for passengers and the crew to continue the travel as soon as possible and also the restitution without delay of the aircraft and its cargo to those to whom they belong by virtue of law;

c) measures undertaken in respect of the suspected author of the offence and, particularly, the result of an extradition procedure or of any judicial procedure [3, article 11; 2, article 13].

In the same sense, if any of contractor states has the reason to suppose that an offence stipulated in conventions will be committed, it transmits, according to the provisions of its national legislations, all the useful data it possesses to states considered enlisted in the requirements of competence.

Taking into consideration the possibility of some disagreements between the contractor states, provisions that would contribute to the solution or would prescribe the mode in which disagreements would be solved were included. Thus, any disagreement between the contractor states in connection with the interpretation or the application of convention, which cannot be solved by negotiations, is submitted to the arbitration, at the request of one of these states. If during a period of 6 months from the date the request of arbitration was submitted the parts do not agree on the organization of arbitration, any of these states can submit the disagreement to the International Justice Court, formulating a request according to the Statute of the Court.

Referring to the Convention on the Suppression of Unlawful Acts relating to International Civil Aviation, signed at Beijing on 10.09.2010, and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, concluded at Beijing on 10.09.2010, we would like to mention some aspects of primordial importance which, in our opinion, can contribute to the essential growing of possibilities for the prevention and counteracting of illicit acts against civil aviation security. Thus, a more distinct delimitation of the circle of participants at offences governed by the scope of activity of the international legal acts mentioned above was carried out, referring not only to the authors of offences, but also to the organizers, co-participants and accomplices [7, paragraphs 2,3,4,5 of the article 1].

An aspect of novelty, stipulated in the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft consists in putting forward the idea as if the contractor states, according to the principles of the internal law, can adopt necessary measures to bring to responsibility the legal body located on its territory or founded according to its laws, in case of perpetration by the natural person responsible for the administration of the legal body or for the control of its activity. Such a liability may possibly have criminal, civil or administrative nature. The necessity of guaranteeing that the applied judicial-criminal, civil or administrative punishments are efficient, duly to the culpability and disposing by a negative covenant character is stipulated as an essential condition. In the cases mentioned above can be applied sanctions by a financial character. Also, the liability of the legal body does not exclude the application of punishment of the natural person guilty of committing the specific crime.

In general, Conventions adopted with a view of regulating situations which could have an impact on the security of the civil aviation, generating serious negative consequences, attempting to the social values and social relations that have to be protected by the national criminal legislation, are induced by the necessity of taking some complex measures orientated to the preventing and combating criminal phenomenon which attempt to the field of regulation of mentioned legislative instruments. Besides, the adoption of the analyzed Conventions was aimed at enhancing the effectiveness of cooperation between the contractor states and ensuring the possibility to use sanctions against persons involved into the perpetration of offences against civil aviation security.

With a view of adapting to the time requirements, the Republic of Moldova undertook a range of actions for fortifying measures aimed at ensuring the security of the aeronautic transport. The first step undertaken in this sense was including into the national Criminal Code of article 275 “The hijacking or the seizure of a train, of an aircraft, a sea craft and a river craft”. It stipulates the liability for the facts described in the provision of the article and also in the presence of some qualifying signs in case some serious and very serious consequences appear.

Along with the great number of technical and organizational measures, necessary statutory acts were adopted for the increasing of the aeronautic security and for the security of airports. Between these there is the adoption by the Parliament of the RM of the Law no 136-XVI as of 19.06.2008 (Official Monitor nr. 145-151/591 as of 08.08.2008) trough which amendments and additions to the Criminal Code of the RM were operated. Thus, for the implementation of the requirements of the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on 23 September 1971[1], the criminal legislation of the Republic of Moldova was supplemented with the article 289[1] “Crimes against the aviation security and against the security of airports”.

The following actions that may possibly endanger the aviation security and the security of airports can be deduced from the article mentioned above:

a) perpetration of an act of violence against a person on board of an in-flight aircraft, if this act may possibly endanger the security of the aircraft;

b) perpetration of an act of violence against a person being in an airport that serves civil aviation, if this act may possibly endanger the security of the airport;

c) destruction of an aircraft being in use or causing damages to the aircraft, which can make it inoperative or can endanger the security of the in-flight aircraft;

d) placing or other act that leads to placing on board of an aircraft in use, by any method, of an apparatus or a substance that is capable to destroy this aircraft or cause damages, which can make it inoperative or can endanger the security of the in-flight aircraft;

e) destruction or damage of equipment or air navigation system, or perturbation of their functioning, if these actions may possibly endanger the security of the in-flight aircraft;

f) destroy or damage of the equipment or the facility of the airport, that serves civil aviation, or of an aircraft stationed in an airport and that is not in use, or perturbation of the activity of the airport services, if these actions may possibly endanger the security of the airport;

g) report of a wrong information, knowing that it is false, if it may possibly endanger the security of an in-flight aircraft;

Paragraph (2) of the same article stipulates punishment for the same actions that by imprudence led to:

a) serious bodily or health injury;

b) death of a person;

c) other serious consequences.

Paragraph (3) specifies the liability for the perpetration of acts stipulated in paragraph (1) or (2), committed by an organized crime group or criminal organization.

Any liable natural person that has reached the age of 16 at the moment of the crime perpetration may appear as a subject of the abovementioned corpus delicti.

As article 289 has been introduced into national criminal legislation before 10 September 2010, when the Protocol Supplementary to the Convention for the Suppression on Unlawful Seizure of Aircraft was adopted, there are certain aspects, which cannot be found in the Criminal Code of the Republic of Moldova. Thus, we consider that some acts described in paragraph 1 of the art. 289 of the Criminal Code can be committed with the involvement of legal bodies or by using their possibilities. In this regard, it would be reasonable to hold legal bodies criminally liable for the perpetration of the above mentioned offences.

Finally, with a view of summarizing the above, it is worthy to stress the importance of some legal levers that would ensure the possibility of preventing and fighting these illicit acts directed against the security of the civil aviation. An accurate governing of this field can improve the safety level in the process of serving civil aviation, at the same time avoiding serious consequences, as damaging aircrafts, their use for terrorist purposes, detention of passengers and members of crew as hostages, threatening their life and health. In addition, by the implementation of these measures the security level of aircrafts and airports will increase, in this way augmenting trust in this kind of transport.

"Is a European Union Intelligence Service (EUIS) Needed?"

Prof. John M. NOMIKOS[*]

Abstract

The end of the Cold War has created a world in which the relative stability between the two superpowers has disappeared. Today, terrorism referred to as the world's second oldest profession, has moved to the top of the international political agenda. It has replaced the Cold War as one of the main security threats – at least in the perception of many in the developed world. Nowadays, the European Union is facing significant new security threats such as illegal migration, human and drug trafficking, transnational organized crime, right wing extremism, Islamic networks, WMD and terrorism. A European Union Independent Intelligence Agency is needed for various reasons. For the provision of security through intelligence directed straight for and by the European Union. In order for the European Union to reinforce its position as a global power, it needs an independent agency from outsiders for its intelligence. It is a delicate process, which should take into account the problems caused by the nature of "intelligence sharing." Without a comprehensive intelligence and firm policy, terrorism, ethnic and religious conflicts, will continue to present a real threat to our transatlantic values in the 21st century.

Keywords: EU, intelligence service, cooperation

The end of the Cold War more than a decade ago created a world in which the relative stability between the two superpowers has disappeared. During the Cold War, a country's every action was conducted in the light of the adversary relationship between the United States and the Soviet Union. The cataclysmic changes that took place in Central and Eastern Europe inevitably changed the face of politics in Europe and in the Western world as a whole. The civil war in Yugoslavia was, and continues to be, the first case of ethnic conflict in Europe in the post-Cold War order.

On 11 September 2001 (9/11), the international community was introduced to a new type of terrorism, one that was truly global in its organization and its impact. In both the European Union (EU) and the United States (USA), it was immediately clear that an effective response would require new levels of cooperation across

[*] Director of the Research Institute for European and American Studies (RIEAS) and Founding Editor, Journal of Mediterranean and Balkan Intelligence (JMBI) based in Athens, Greece

the Atlantic and around the world. The post 11 September 2001 era has challenged governments, policymakers, religious leaders, the media and the general public to play both critical and constructive roles in the war against global terrorism[1].

During the 1990s, the European Union has kept a relative low profile in the world and European arena. As with the USA in the post WWII era, the European Union has had little to no experience in dealing with these new problems. In July 1991, the European Union had to deal with a major crisis in Yugoslavia that led to tragic civil war. The European Union member states did not realize how deep-rooted the conflict between the different ethnic groups was. Though continuous analysis of the situation, the European Union member states might have been able to realize sooner that a major conflict in Yugoslavia was inevitable and been able to diffuse the conflict before it could explode[2].

The Treaty of Maastricht negotiated by the EU in 1991 helped set the agenda, establishing as EU objectives the implementation of a Common Foreign and Security Policy (CFSP) as well as the eventual framing of a common defense policy. There were no means established to implement a CFSP, however, nor did the Treaty of Maastricht make any specific mention of increasing intelligence cooperation with the CFSP framework[3].

Most important, at the British – French Summit at St. Malo (1998), it was stated that intelligence was fundamental to the success of the European Union, and that it must be given appropriate structures and a capacity for analysis of situations, sources of intelligence, and a capability for relevant strategic planning without unnecessary duplication. This notion was also reinforced in the Amsterdam Treaty (1997) in order to create a policy of planning and early warning unit[4].

Moreover, Intelligence and security analysts in the European Union member-states who promote the idea of a European common intelligence policy argue that intelligence collaboration is already taking place successfully around the world; in the EU Satellite Center in Spain; the Situation Center at the United Nations in New York and the informal gathering of the Club of Berne in Switzerland[5]. However, the toughest challenge for the European Union has been the highly sensitive area of intelligence-sharing. The European Union has decided that from January 1, 2008, any information available in one country should be available in all other 27 member-states.

The tentative European intelligence cooperation that developed during the 1990s fell short of a common policy necessary for an effective Common Foreign and Security Policy (CFSP) and autonomous defense capability. European intelligence cooperation to date has been hampered by emphasizing national sovereignty over sharing intelligence. Institutional obstacles also stand in the way of increased intelligence cooperation[6] Intelligence organizations generally believe that no other organization's analysis is as reliable as their own, which leads them to place more faith and confidence in their own work. These organizations also tend to view International Relations as a zero-sum game, and may not agree with a cooperative approach to security and defense integration.

The Persian Gulf and Yugoslavia crises proved more of an impetus to a common European Union Intelligence cooperation policy than did Maastricht. Dependence on the United States for intelligence during both crises convinced the Europeans that they needed improved intelligence collection capabilities, especially with regard to space-based assets.

Analyzing the role of a prospective European Union Intelligence Service (EUIS)

To be effective a European Common Intelligence Policy must be able to swiftly and accurately disseminate intelligence information to military forces. The ability to do so is crucial to the development of a European Intelligence Policy, as well as the multinational corps agreed upon in Helsinki Summit[7].

However, how a European Union Intelligence Service (EUIS) might fit in the overall European Union mechanism and what its shape and role might be, is a prospective challenge for the member-states in the European Union. Its most important task would be the analysis of overtly gathered information and preparing it for use by the policy-makers. The question of to whom the European Union Intelligence Director will report, should be a compromise among the European Commission, European Council and the European Parliament.

Furthermore, when the European Union Intelligence Service (EUIS) foresees a situation which could be threatening to the EU member states, such as the crisis in Yugoslavia or prospective religious turmoil leading to terrorist acts, the Council of Ministers should be involved as well by informing appropriately their national intelligence services.

Since the Council of Ministers is the official decision-making body of the European Union, it should receive reports and analysis from the European Union Intelligence Service. However, the problem here is that a Minister of foreign affairs might have difficulties and conflicts in dealing with the foreign affairs of his own country and that of the European Union at the same time. This is a good reason to found a *Committee on European Intelligence*, which will refer directly to the EU Commission.

On the other side, the European Parliament would be the one to approve the budget of the European Union Intelligence Service. In the U.S., the Congress is also responsible for the approval of the budget of the United States Intelligence Community. The European Parliament could in the future also become the institution to provide oversight over the European Union Intelligence Service operations comparable to U.S. Congressional oversight over the Intelligence Community.

In addition, the Council of Ministers as well as the European Parliament could also be involved in the determination of the issues that should be monitored by the European Union Intelligence Service (EUIS).

However, threats have to be clearly identified and a European Common Foreign and Security Policy (CFSP) must be corresponded to a coherent intelligence action that would be defined in a *European Intelligence Act*. This act would support the pillar's role of the European Director of Intelligence in a renewal transatlantic cooperation within the framework of North Atlantic Treaty Organization (NATO).

Concluding remarks

European intelligence cooperation to date has been hampered by emphasizing national sovereignty over sharing-intelligence. The cooperation that does exist has been largely confined to imagery collection and analysis using the European Union Satellite Center (SATCEN). Imagery intelligence is a necessary capability, but an effective

European Union Intelligence Service (EUIS) will require collaboration in signals intelligence (SIGINT) and human intelligence (HUMINT), and be able to integrate them in all-source intelligence products.

The tragic events in Madrid (2004), London (2005) and Burgas (2012) have initiated a discussion about the poor state of the European counter-terrorism cooperation. Alongside the discussion, a concept to create a European Union Intelligence Service (EUIS) has arisen. However, it seems that to ascribe the issue only to counter-terrorism prevention is misleading and is also making it difficult to define matters of the European intelligence cooperation in its right place and context, namely as an indispensable mechanism for implementing Common Foreign and Security Policy (CFSP) and European Security and Defense Policy (ESDP)[8].

By forming an intelligence service, European Union member states would be able to foresee prospective conflicts in the European continent since the international order has changed dramatically in the last years and has not made the world more stable. The Balkan and Mediterranean region is an area with considerable instability and increasing of threats such as illegal immigration, human trafficking, Islamic networks, and terrorism-organized groups collaboration. European Union member states have consequently become more active in the international arena (Afghanistan, Iraq, Syria and Arab Spring in the North Africa states). A lack of knowledge about other potential conflicts in the region could be more costly than maintaining a viable European Union Intelligence Service (EUIS).

The EUIS's main tasks would be gathering information from the EU member states' intelligence organizations and *analyzing it independently*. This analysis would allow the EUIS to advise the Commission and the Council on foreign relations and security issues. Most of the information needed for thorough analysis would be obtained overtly.

At the end, the European Union member states need to understand that terrorism, transnational organized groups and Islamic networks is an international problem, not a European one and it requires more than ever collective action among the intelligence services depending on shared intelligence and common assessments in order to prevent prospective major terrorist acts in the European continent!

References

[1] John M Nomikos, "The Transatlantic Intelligence Cooperation, the Global War on Terrorism, and International Order" in Yannis A. Stivachtis (ed) *International Order in a Globalizing World*, (London, UK: Ashgate Publishing Ltd, 2007), pp: 161-181.

[2] John M Nomikos, "European Intelligence Cooperation Beyond the Nation State: A Prerequisite for Common Foreign and Security Policy (CFSP)",in http://worldsecuritynetwork.com/Other/john-nomikos-1/European-Intelligence-Cooperation-Beyond-the-Nation-State-A-prerequisite-for-common-foreign-and-security-policy-CFSP, World Security Network Foundation, Germany, 2006.

[3] John M Nomikos, "European Union Intelligence Agency: a necessary institution for Common Intelligence Policy?", in Vassiliki Koutrakou (ed), *Contemporary Issues and Debates in EU Policy*, (Manchester UK: Manchester University Press, 2004), pp: 47-48.

[4] John M Nomikos, "EU Intelligence Cooperation: A Greek Approach", in http://www.europeanbusinessreview.eu/page.asp?pid=851, *European Business Review*, Athens, Greece, 2010.

[5] *Ibid*.

[6] *Ibid*., John M Nomikos, "The Transatlantic Intelligence Cooperation, the Global War on Terrorism, and International Order", 2007, p: 169.

[7] European Union leaders meeting in Helsinki, (December 1999), and a follow up meeting in Sintra, Portugal in February 2000 agreed to major changes in European security and defense policy, many of which had been initially suggested in Cologne, Germany. Three additional boded have already been established to support the European Union Defense Policy: a Political and Security Committee, composed of ambassadors with an advisory role to the EU Council of Ministers; on EU Military Committee of senior officers; and a Multinational Planning Staff. While details of the intelligence support to be provided to the multinational force are not yet available this level of support is likely to require significantly increased intelligence collaboration.

[8] Antoni Podolski, "European Intelligence Cooperation: A Failing Part of the CFSP and ESDP?", *Euro Future Journal,* pp: 44-47, Paris, France, 2005.

Conceptual Challenges Towards Intelligence Quality in the Knowledge Society Framework

Valentyna PANCHENKO[*]

Abstract

The article analyses the main attributes and features of data, information, knowledge and wisdom. The role and tasks of intelligence agencies in the knowledge-based society are discussed. The global trends of modern society transformation and their influence on intelligence agencies activity are determined.

Keywords: data, information, knowledge, wisdom, intelligence, knowledge-based society

The rapid development of information and communication technologies as powerful tools for data, information and knowledge processing greatly accelerated social transformations that were predicted in the 60s of the last century by prominent philosophers, sociologists and political scientists. These theories were dedicated to post-modern society (D. Bell), information society (Y. Masuda, A. Toffler, M. McLuhan) and knowledge-based society (V. Vernadsky, P. Drucker, F. Machlup). They assumed the strategic perspective that a certain group of countries significantly would strengthen its role in global processes due to priority of the newest knowledge production and using, thereby increasing the life quality and safety of its citizens. The rest of the countries that do not possess these skills and tools would become more dependent on the first group and would pay for the good of civilization by cheap labor and natural resources, environmental quotas and other national security components.

Intelligence is directly related to information activities, therefore is sensitive to these changes. Under the conditions of the knowledge society formation taking into account the new principles of social development is extremely important for the national security of any country and for preserving the competitiveness of its intelligence agencies.

[*] PhD in Engineering, National Academy of Security Service, Ukraine

Thus, the purpose of the study is to determine the conceptual challenges towards intelligence quality in the knowledge society framework as well as features that must be considered by intelligence agencies even currently to be ready for new social transformations.

Information society *vs*. knowledge-based society

Today we live in the information society. The evidence is the fact that we do not trade in goods but in brands. It means that, for example, buying from an online store two tables for a notebook from different producers in different countries at different price, you may find out that you have purchased quite similar ones in form and functions gadgets made in China. The difference between them would be just in the name of the brand: the inscription "Maxxtro" on the one and "UFT" on the other.

Another indicator of the information society is be considered by the survey of experts in 2013 at the World Economic Forum in Davos the recognition of information inequality (between the developed countries and the rest of the world and within countries between different sectors of the population) as one of the most serious problems of humanity, along with economic and digital inequality.

At the same time the analysis of scientific publications affirms that conversation about knowledge society or knowledge-based society emergence are premature. The question is whether all types of societies that have changed over evolutionary history are characterized by the elaboration and use of new knowledge for their own development. But since the 80-90^{s} of last century we note the new qualitative features in the process. Mankind overcame means of converting information into digital form, created a large repository to store it, passing it at a distance using information and communication technologies. This led to a fundamentally new interaction between people. Since the second half of the nineties information began to act as a commodity which can be bought and sold. But at the same time it has not become a sufficient resource for the harmonious development of society, only just raw material processed before using. This kind of society was called "information society". It is characterized by a massive output of information, information is the most valuable resource and its availability is one of the most important principles of social interaction. Thus, the information society is based on information technology and information goods exchange in the whole world.

Such a society is beginning to provide a high economic development of individual countries and multinational companies, but does not guarantee the life quality or security of its members. Because information inequality leads to a deepening economic inequality. Therefore, there is an urgent need for groundwork and keeping strict regulations both globally and within countries that would have political and economic instruments of social development for the benefit of people, ensuring quality and safety of their life rather than reducing these fundamental values.

The concept of forming a new type of society emerged at the turn of the century, when information began to acquire a qualitatively new form – the harmonized knowledge, providing the ability to overcome the internal and external contradictions in society. This form of society, so called knowledge-based society or knowledge society, allows a person to move to mass production of new knowledge using powerful tools like information and telecommunication technologies.

In contrast to the information society, knowledge society aims to achieve cognitive outcomes rather than process. The society of this kind is entirely of new dimension, which, in addition to technology, is social, spiritual, ethnic and political. Integral components of knowledge society must be new interdisciplinary knowledge, which generate scientific and technical institutions, provide training of highly qualified personnel, produce additional resources on the basis of the knowledge economy and forming an integral development vector of society, aimed to improve the safety and life quality for all its members. The logic of this reasoning is that the free access to knowledge and sharing will help to strengthen open public institutions and tolerant dialogue. In such a society one of the best values is the training and skills to effectively use information, the role of information technology is to facilitate continuous updating of personal and professional competence.

In view of the above, we can reach the following conclusions: 1) knowledge society today is more an ideal model than real existence, and 2) we can observe fundamental differences between the information society and knowledge society. Does this mean that in a knowledge society fundamentally new challenges for intelligence will emerge?

DIKW model

To answer this question, we must turn to the nature of the concepts of information and knowledge. In our view, the differences between these concepts best describes DIKW model (data, information, knowledge, wisdom).

According to this model the data is the facts presented by numbers, symbols and signals. They simply exist, and exist in any form, usable or not.

Information - is interpreted facts, ie, data organized in a certain way, depending on the objectives, needs and knowledge of the subject, their processing. Thus, different entities (organizations, individuals, etc.) can have available the same information, but the information they gain from these data may be different depending on their education, age, social and professional status and intended use (to improve the overall scholarship, solving scientific, technical, industrial, commercial problems). The data for one subject looks quite accurate and complete to the other - can be wrong and scattered. The mistake people make is thinking that the information they are looking at is always an accurate reflection of the data.

So information is always subjective. For example, the main characterizing features of intelligence are: novelty, timeliness, completeness, accuracy and compliance objectives, reliability, availability perception. Some scholars further distinguish such important characteristics of intelligence as time costs of obtaining it, the cost of time to study the information, objectivity, importance (requires an immediate response, important to national security, not directly affect the security situation).

Information becomes knowledge if it contains no ambiguity and has a regular character. Hence, knowledge is selected, resulting in a certain way, orderly, decorated set of information that can be repeatedly used for decision-making. Knowledge does not allow subjectivity as prompted by repeatedly proven facts. However, even stable knowledge of the objective laws of nature are valid as long as the new surveys did not obtain new knowledge (eg, the laws of Isaac Newton). Thus, knowledge is characterized by the great terms of moral depreciation.

Wisdom is applied knowledge, whereby deriving rules for the knowledge generation (for example, a first grader has knowledge that 2x2 = 4, but he can not calculate 342x45 because doesn't know the rules by which multiplication is performed). Wisdom allows you to identify patterns and provides an answer to the question of how and where to apply the knowledge.

In general, the DIKW model can be displayed as follows (Figure 1).

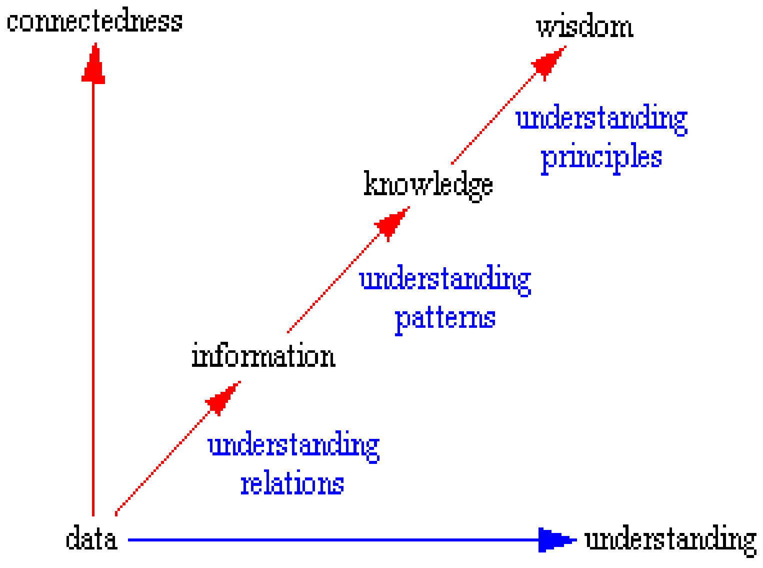


Figure 1 – DIKW model

So, the data form is signals and symbols convenient model for data representation is the table. Information is always structured, subjective and functional. The best model for information is a graph. Knowledge is a procedure or process and the most appropriate model for it is a graph. Wisdom allows you to create proposals what to do. In our view, the model of wisdom is a neural network because it helps to understand the rules. Example of data, information, knowledge and wisdom are presented in Table 1.

Table 1

Example of data, information, knowledge and wisdom

Data	Ukraine's GDP in 2012 reached 176.3 billion dollars
Information	Compared to 2011 Ukraine's GDP grew by 6.7% in 2012
Knowledge	Provided the previous trend we can expect Ukraine's GDP growth by 2.2% in 2013
Wisdom	Given the steady increase awareness of GDP in Ukraine, other financial indicators as well as the tendency to reduce corruption, we consider it possible to invest in the Ukraine economy

Considering the features of the nature of concepts of "information" and "knowledge" we can reach the following conclusion: in the knowledge society data will remain with its inherent properties, information will remain as information, and knowledge will remain as knowledge. The basic properties of intelligence (novelty, timeliness, completeness, accuracy and compliance purposes, the availability of perception) in the knowledge society will remain unchanged too.

What can change in a knowledge society?

The amount of data will continue to grow, it will become more accessible (open). So if a few years ago the Internet was the source of a socio-political data only, with the advent of social services today we can access personal data too. Therefore, in a knowledge society will not be a question how to obtain information instead it will be a question how to obtain knowledge from the information.

How to solve the problem of data growth?

First, the rapid development of information and communication technologies caused increasing the amount of data, so technologies and systems for information processing focused on gaining knowledge should be used to solve this problem.

In our opinion, today information systems, based on different forms of knowledge representation are successfully proven:

1. Expert systems that contain data and the rules by which the data are processed. For example, it is known that women in working hours have many short-term talking on the phone while on weekends and in the evening their conversation last long. Men do not talk long on the phone. Using this rule and collected data on telephone calls of offender in an expert system we can establish its gender.

2. Wiki-projects provide an opportunity to accumulate encyclopedic knowledge. Also, interesting information can be obtained by analyzing the language data in the multilingual versions of Wikipedia or the themes of its the most edited articles in different countries.

3. Ontological systems provide the opportunity to accumulate knowledge, discover hidden relationships between objects of different nature. Example of a graph for displaying objects (businessmen, politicians, political and financial organisations) of the socio- political news of Ukraine by ontologically oriented model are presented in Figure 2.

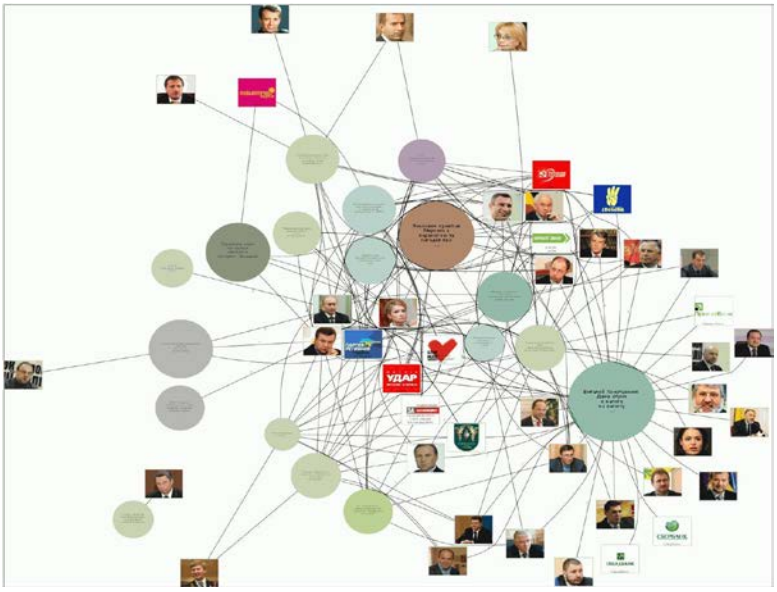


Figure 2 – Example of a graph for displaying objects of the socio-political news of Ukraine by ontologically oriented model

Secondly, continuous learning and transformation of information into knowledge have become key competencies of a specialist who deals with the intelligence in a new society - a society of knowledge. The ability to navigate the flow of information, cognitive properties, critical thinking, which help to distinguish useful information from "noise" will be more and more important.

So unlike material goods, information can be shared with the world via the Internet almost free. Someone considers the Internet as a new socio-political system - democratic, horizontally structured, self-organized, non-hierarchical, open and interactive. However, the growth of communication network itself does not contribute to the creation of a knowledge society. While the price of information reproduction can be low, reproduction of knowledge is much more expensive process, because it is difficult to determine the minimum required amount of knowledge to transfer it to other subjects. In addition, the process of learning effectively takes time. Therefore, in a knowledge society ability of lifelong learning becomes an essential requirement to a specialist in the information analysis area. The modern education systems with their traditional framework of constant training will not be sufficient to satisfy the requirements of knowledge society. Therefore, it is appropriate to create opportunities for continuous professional development at all stages of professional development.

Conclusions

Today a new type of society, the society of knowledge, is forming. It is assumed that due to knowledge mankind can overcome the conflicts and contradictions, and to direct its potential for spiritual, economic and technological development. So the knowledge society will set new challenges for intelligence agencies. Their main context is to obtain intelligence in the interests of security (harmonious development, social protection, improving the welfare) of the population of their own country by gaining new knowledge, rather than by reallocating resources (raw materials, human, informational) of other countries.

Thus, in a knowledge society intelligence agencies should focus on obtaining knowledge as the main form of intelligence that will act as a basic requirement towards its quality. In order to fulfill this task intelligence agencies should already implement the information systems based on knowledge, and improve intelligence education system to provide the formation of core competence - transforming information into knowledge.

References

1. Шлях до суспільства, заснованого на знаннях, accessed 29 June 2013 at http://kpi.ua/605

2. Давос: «Глобальні ризики-2013», accessed 29 June 2013 at http://uaforeignaffairs.com/ua/ekspertna-dumka/view

3. Опенков М.Ю., *Хакни будущее : введение в философию общества знаний* (Москва: МОО ВПП ЮНЕСКО «Информация для всех », 2007), с.128

4. Савченко И.В., "Информационное общество или общество знаний?", научный журнал, *Современные наукоемкие технологии*, accessed 29 June 2013 at http://www.rae.ru/snt/?section=content&op=show_article&article_id=5081

5. Програмні засади розбудови суспільства знань: світовий досвід для України accessed 29 June 2013 at http://old.niss.gov.ua/Monitor/may/9.htm

6. Ефременко Д.В., "Концепция общества знания как теория социальных трансформаций: достижения и проблемы", научный журнал, *Вопросы философии*, accessed 29 June 2013 at http://vphil.ru/index.php?option=com_content&task=view&id=91&Itemid=52

7. Gene Bellinger, Durval Castro, Anthony Mills, "Data, Information, Knowledge, and Wisdom", accessed 29 June 2013 at http://www.systems-thinking.org/dikw/dikw.htm

8. Общественно-политические новости: сюжетный паттерн, accessed 1 July 2013 at http://wwell.com.ua/wwell.php?ln=ru&date=20130910&h_menu=main&h_submenu=&sr=SBJ00000&section_cold="&msg_id=News/wwell_20130902_1115.xml