ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 14
December
2015

Journal with scientific prestige acknowledged by the National Council for the Validation of University Titles, Diplomas and Certificates (CNADTCU), indexed in the international databases CEEOL and EBSCO

Bucharest
- 2015 -

Senior Editors

Board of Editors

..

CONTENT

INTERNATIONAL SECURITY ENVIRONMENT

THE DEVELOPING GLOBAL CRISIS AND THE CURRENT WAVE OF MIGRANT/REFUGEES HEADING FOR EUROPE

Michael ANDREGG[*]

Abstract

A "Developing Global Crisis" is unfolding today that reflects synergistic interactions among demographic pressures, authoritarian politics, militant religion, corruptions of governance and other factors worldwide. All of these four and several other relevant factors are complex, and many interact synergistically (e.g. non-linear interactions) so they will be illustrated by the case of Syria here.

Keywords: global crisis, migrant, Syria, demographic pressure**.**

Introduction

A "Developing Global Crisis" is unfolding today that reflects synergistic interactions among demographic pressures, authoritarian politics, militant religion, corruptions of governance and other factors worldwide. All of these four and several other relevant factors are complex, and many interact synergistically (e.g. non-linear interactions) so they will be illustrated by the case of Syria here. Much commentary on that crisis focuses on the personalities of Bashar al-Assad and Vladimir Putin of Russia. Other observers focus on emergent forces of evil like the death cult ISIS (ISIL, Daesh or Islamic State – the name does not matter here) – or their leaders.

These are all relevant to many questions, but they can obscure ultimate causes of war like the demographic pressures that generate so many global problems today, and pervasive corruptions of governance that prevent solution of them. For example, before the current crisis, the population growth rate in Syria was about 2.4% per year which yields a doubling time of less than 30 years (CIA World FactBook, 2010). That puts enormous pressure on natural resources like farmland and water. Climate change is a derivative factor caused by population growth and industrial development. Syria endured its worst drought in 150 years (recorded history of rainfall there) for four years before the conflict began. The World Bank reports that at least 1.5 million people (8% of Syria's population) left unproductive rural areas for cities that were already overburdened with millions of unemployed youth (Liverani, 2015). Sources on

[*] Michael Andregg teacher in the Justice and Peace Studies Department at the University of St. Thomas in St. Paul, Minnesota, USA.

the ground have claimed even more to me. These internal migrants poured into cities bereft of opportunity for already large teenaged populations. Another effect of high birth rates is pyramidal age distributions with many youth compared to elders.

Assad reserved the best opportunities for his Alawite prime constituency and for minority allies like Christians. Peaceful protests began in cities over lack of opportunity for the rest, and other corruptions. Security institutions over-reacted and repression morphed into civil war(s). Even if Bashar al-Assad had been an angel of God (or a potted plant) he would have been faced with a wicked problem.

Caught between barrel bombs, chemical attacks and forced conscription on one side, and ISIS or Al Qaeda on the other side, millions of people fled into Turkey, Lebanon and Jordan, putting great pressure on those countries also well over 4 million, with another 8 million internally displaced (UNHCR, August 29, 2015). In time, the richer, better educated and more entrepreneurial decided that a life in refugee camps was not acceptable for their children. So a trickle of migrants into Europe became a river. When Angela Merkel announced that Germany would welcome hundreds of thousands of them, the river became a flood (Wagstyl, 2015). This will not end soon, and this is not just a German or even a European issue. Note how long North America has struggled with mass immigration from the south, and how paralyzed US politics has become on these issues.

Following sections will provide more detail on some of these factors. But the bottom line deserves emphasis now. "Solutions" to crises like this that do not at least acknowledge root causes like:

a) Population pressure;
b) Climate change;
c) Authoritarian law;
d) Militant religion;
e) Corruption of governance;
f) Income inequalities within and between nations, and
g) The special power of demagogues in conditions like this to mobilize the desperate by focusing their anger on easily identifiable others, are doomed to fail.

This will be a generational problem with very large consequences for the whole world. Add weapons of mass destruction, and taboos on discussing many of these factors, and you have what some have come to call a "wicked" problem[1].

Population Growth, Population Pressure and Climate Change

[1] For a definition of "wicked problems" see https://en.wikipedia.org/wiki/Wicked_problem.

Population growth and population pressure are not the same thing, but both increase competition for resources. If resources become scarce, some people are always tempted to fight over access to them. If critical resources become very scarce, many people will support wars of their group against others. If starvation is imminent, even sophisticated, "civilized" people may fight over bread, or steal from wealthier neighbours. Climate change is a derivative factor, a consequence of centuries of population growth on earth and reliance on fossil fuels to power our societies. It has become quite clear that increased levels of carbon dioxide in the air and other by-products of burning oil, coal, gas and forests are causing significant increases in global temperature that have other consequences for marginal populations and even for the living system that sustains us all.

How many people can thrive on any particular area of land is very dependent on the technology available to those people and the quality of that land. Population growth is simple arithmetic, absolute numbers of people, birth rates, death rates, fertility rates, doubling times, net migration and similar numbers (Andregg, 2014). A high-tech society on fertile land can support many more people than could be fed on the same land with 19th century agriculture. So **population pressure** reflects economic, technical and cultural factors among many others. No matter how fertile, all land has limits and none can support endless growth. That is elementary ecology. But societies often resist this basic law of nature. If a society keeps growing once those limits are reached, there is increasing pressure for some people of the society to expand into neighbouring lands, or just to move there. Vast though it is, our earth is finite. And every culture on earth has fears about being overwhelmed by such migrants, because this has happened many times in human history.

Climate change matters today because we already have over 60 million permanent refugees on this earth, most of whom have fled violent conflicts in their nations of origin (Mocanu, October 17, 2015). Hundreds of millions more are on the move, migrants of one kind or another. Reports like the annual report of the Intergovernmental Panel on Climate Change (2014) indicate that as the earth warms droughts will become more common in many places, flooding in others, storms will become more energetic on average, and oceans will acidify as CO2 is absorbed, and rise as glaciers and polar ice melts. This has vast implications for international security. Syria is one example.

Authoritarian Law and Militant Religion

Authoritarian Law is not the same as Militant Religion, but they both increase the probability of organized armed conflict in several ways. As importantly, they react synergistically such that both in combination are more dangerous than either alone. I dealt with this in more detail in a book on the causes of war in 2001 (Andregg, 2001, chapter 13, pp. 74-83), but the essence is that authoritarian law provides the practical means for political repression or conquest, with or without justification, while militant religion provides "moral" rationales for the use of state violence against others. Consider ISIS for a current and extreme example. But there have been many other moral crusades against designated others in history based on some theory of religion (like, the Islamists often point out, the medieval "Crusades" to "free" Jerusalem during the 11th – 13th centuries CE).

In the Syrian case, the government of Bashar al-Assad always was authoritarian (his father Hafez infamously killed an estimated 20,000 people in Hama in February 1982 for resisting his rule). That authoritarian law legitimized violence, and funded well-armed police and soldiers who repressed the early protests in 2011. After years of abuse, ISIS arose on the principle of militant religion, claiming that the regime was an agent of Shaytan (Satan) and that "good Muslims" had a responsibility to attack that evil regime. And if you are Muslim but don't agree, well you are a "bad" Muslim, subject to execution. There is no middle ground with ISIS; you are with them or against them, but cannot be neutral. The current ISIS leader, Abu Bakr al-Baghdadi, takes this goal and style to its limit by claiming a mission from "god" to rule everyone on earth under a "new Caliphate".

Either factor is very dangerous. Put the two together and you can get intense reactions, like sodium with water, because both authoritarian law and militant religion intend to be the *only* legitimate user of violent methods. They cannot tolerate each other, and innocents in their territories are always at risk. The most dangerous of all is when religious moral zealotry and authoritarian political power fuse. Those dictators think they are actually God's designated rulers of the earth. Such people know no shame in their abuse of others to "accomplish god's will". This provides extremely fertile ground for "demagogues", a particularly dangerous type of political personality. We will cover that briefly after the section on corruptions of governance.

Corruptions of Governance and Income Inequalities

Corruption of governance has been with us since the beginning of time, but it is among the least studied basic causes of war. The main reason for this is that most funding for social science comes from governments, which are generally not pleased by people studying corruption of governance. In the context of this paper, this factor is important because it prevents many governments from solving obvious and sometimes even lethal problems for their peoples.

Income inequality is also global and eternal, and is more obviously related to the civil wars that predominate today. The case of Syria is actually a small example of a very global problem. In general, the probability of conflict increases with income inequality, both within and between nations. These topics are too complex for a simple review, so I will illustrate them very briefly with how both factors affect external actors, specifically the US response to the Syrian crisis.

As the civil wars unfolded and metastasized in Syria, the USA wondered what to do. But its frame of reference for understanding the conflict had to be military. And because of our own domestic political dynamics, it had to focus on personalities like Bashar al-Assad and Abu Bakr al-Baghdadi rather than impersonal forces like population growth, climate change or systemic corruptions of governance. So rather than deal with any of those expensive and very difficult problems, the practical question has been whether to bomb targets, and if so which ones?

In fact, denial of the reality of climate change (encouraged by large investments of money and influence by fossil fuel companies) was so great when things fell apart in Syria that a very large majority of one of our two main political parties were on record as doubting that this was even a problem, despite a Pentagon report as early as 2003 that climate change would have dramatic national and international security consequences (Schwartz & Randall, October, 2003). Such Congressman preferred to think of Syria as a military problem caused by one or more evil leaders in foreign countries. The fact that military responses, especially bombs, have zero positive effect on climate change and no therapeutic value when applied to mass migrations and corrupt governments does not even cross their minds. They prefer simple good-and-evil stories. Meanwhile, failures of US policy pile up along with failed states in the Middle East, while forces of tribal rebellion against corrupt governments there grow inexorably. Tens of millions of very poorly educated teen aged males are now maturing into desperate circumstances where demagogues are eager to focus their anger.

Demagogues, Psychopaths and WMDs

As with the preceding sections, demagogues are not identical to psychopaths, but they are both common in high politics and dangerous to polite society because they are fundamentally parasitic on societies. Both are especially adept at manipulating gullible people, and ruthless in their methods. They do not produce anything of value themselves, but often focus the anger of desperate people on some easily identifiable "other" usually a minority ethnic or religious group. Where governments are notoriously corrupt, they may be the best target. When the psychopath or demagogue seizes power of a major nation, the target becomes neighbour nations or some symbolic "fifth column" of dual loyalists, like the Jews of Adolf Hitler's Germany.

The best reference I know on psychological evil in high politics is very difficult to read, but I will cite it anyway because of its unusual authorship. It was created by social scientists and psychiatrists in Poland who survived first the Nazi occupation, and then "liberation" and further subjugation by Soviet forces at the end of World War II. So they were VERY highly motivated to understand how evil forces could capture entire nations. The title is *Political Ponerology* and the nominal author is Andrew M. Lobaczewski, who died in 2007 (Lobaczewski, 2008)[2].

WMD's (Weapons of Mass Destruction) are, of course, weapons, not humans. But they matter intensely in this context, because every psychopath on earth would love to have some. One of the defining characteristics of truly evil people, however you label them, is an inordinate desire for ever more power (Peck, Simon & Schuster, 1983). There is no natural limit to that appetite. As Kevin Dutton (2012) notes, psychopaths are often very successful in both high politics and industry due to their exceptional focus, high intelligence, extreme ability to manipulate "normal" people and general indifference to moral norms especially prohibitions on hurting people. Pure, clinical psychopaths appear to be incapable of empathy, lack compassion and possibly conscience of any kind.

In the case of Syria, there can be little doubt that Abu Bakr al-Baghdadi is a demagogue and possibly a psychopathic leader of a death cult, empowered by the general chaos in failed state Iraq and the similar distress in Syria which has become their main power base. Bashar al-Assad responds, and who actually killed the first innocents becomes an academic question more than a practical one. If either leader had nuclear or other weapons of mass destruction they would use them against their enemies. That brings attention from those who actually do have nuclear and other WMDs.

Conclusions

[2] Is based on a Polish original titled Ponerologia Polityczna published in 1984, translated into English in 1985 by Alexandra Cheiuk-Celt and corrected by the original author in 1998. "Pathocracy" is a term they use to describe nation-states coopted by and often ultimately destroyed by psychopathic leaders. Lobaczewski always maintained that the book was written with many collaborators, mainly social scientists and psychiatrists in Poland who were slowly ground up by the Soviet system as they tried to express their work.

In my opinion, the current wave of migrant/refugees heading for Europe is not temporary, and will not end even in the theoretical event if conditions in Syria improved dramatically overnight. It would be great to achieve a new peace there, as anywhere, but the point is that this is a global phenomenon caused fundamentally by high birth rates among peoples living in lands that are already mostly desert. In fact, hundreds of millions of young men are now maturing in desperate circumstances with very limited job opportunities. They are being exploited by demagogues who promise fantastic rewards to fighters, and even sometimes significant salaries, payable if they live to collect. These conditions prevail not just in Syria, but in large areas of North Africa and the Middle East today, among other places. All of these areas are generating migrants who naturally move along "opportunity gradients" towards prospects of a better future.

Consider for a moment that North America has also seen two generations of significant legal and illegal migration from Mexico and increasingly Central America. They have nothing to do with Syria, and many come from lands which have not yet turned into unproductive desert as lands often do that endure overpopulation for long periods of time. But all seek opportunity, and many flee violence, corruption or oppression in their nations of origin.

So I call the world's attention to these more difficult factors: population pressure, authoritarian law, militant religion, and corruptions of governance, demagogic or psychopathic leaders and the variety of other, derivative factors like climate change and income inequality.

In medicine if you seek cures for major problems it is critical to distinguish between "symptoms" and "causes". Yes, symptoms call for relief. But if one treats only them and neglect cause, like a fever caused by infection, you can cool a patient down and reduce pain but still watch them die. The mass migration out of Syria in 2015 is similar in that it is a symptom of much deeper problems. And the tens of millions of people on the move today do not all come from Syria.

So Europe, like North America, can absorb many migrants productively, and could help many more refugees for excellent humanitarian reasons I support. But it should never lose sight of the fundamental causes of distress in the nations of origin, because no one can absorb unlimited numbers of migrants without significant adverse effects in the destination countries. Help now buys time to deal with the fundamental causes. But if you do not use that time wisely, and fail to recognize or deal with root causes, relief will be temporary while nations of origin are destroyed by the chaos that continues.

References:

1. CIA World FactBook, (2010), demographics of Syria retrieved from https://www.cia.gov/library/publications/download/download-2010.
2. Liverani, Andrea, (October 21, 2015), accessible at: http://blogs.worldbank.org/peoplemove/syrian-refugee-cop21.
3. *United Nation High Commissioner for Refugees, (August 29, 2015),* retrieved from *UNHCR Syria Regional Refugee Response/Total Persons of Concern".*
4. Wagstyl, Stefan, (September 14, 2015), *Merkel's Welcome to Refugees Comes Back to Bite Her*, in „Financial Times", accessible at: http://www.ft.com/intl/cms/s/0/60264684-5af4-11e5-a28b-50226830d644.html#axzz3rDj8NNF.
5. Andregg, Michael (2001) On the Causes of War, 3rd edition, published by Ground Zero Minnesota.
6. Andregg, Michael, (2014) *Seven Billion and Counting: The Crisis in Global Population Growth*, Twenty-First Century Press (an imprint of Lerner Books).
7. Mocanu, Mircea, (October 17, 2015), *Valuing Migration: Benefits and Challenges*, in a paper presented at the 21st annual Conference Information in the Knowledge Society, at Romania's „Mihai Viteazul" National Intelligence Academy, Bucharest.
8. The UN affiliated Intergovernmental Panel on Climate Change Report (2014), available at: http://www.ipcc.ch/report/ar5/syr/.
9. Schwartz, Peter, Randall, Doug (October, 2003) The "Marshall Report" or "An Abrupt Climate Change Scenario and Its Implications for United States National Security", commissioned by Pentagon Strategic Forecasting guru Andrew Marshall available at: http://www.climate.org/PDF/clim_change_scenario.pdf . A good summary of this report's implications can be found at the History Commons, accessed on 11 November, 2015 at: http://www.historycommons.org/context.jsp?item=PentagonClimateChangeReport.
10. Lobaczewski, Andrew M. (2008) *Political Ponerology: A Science on the Nature of Evil Adjusted for Political Purposes*, Red Pill Press, Edmonton Canada.
11. Peck, Scott M., Simon & Shuster (1983) *People of the Lie: The Hope for Healing Human Evil*.
12. Dutton, Kevin, (2012), *The Wisdom of Psychopaths: What Saints, Spies, and Serial Killers can teach us about Success*, Scientific American Press/Farrar, Straus and Giroux.

TERRORISM SERVING GEOPOLITICS. THE RUSSIAN-UKRAINIAN CONFLICT AS AN EXAMPLE OF THE IMPLEMENTATION OF ALEKSANDR DUGIN'S GEOPOLITICAL DOCTRINE AND EVGENY MESSNER'S CONCEPT OF "REBEL WAR"

Michał WOJNOWSKI[*]

Motto:
Without geopolitics it is not possible to understand the events in Ukraine –
every attitude excluding that is doomed to an immediate failure.
(Aleksandr Dugin, March 14, 2014)

Every man, whether a serviceman or a civilian,
takes part in the information warfare no matter of its form.
(Gen. Vladimir Markomienko, 2000)[1]

Abstract:

Defining the interests of the state in reference to its geographical location is the key element to understanding political actions being taken by the Russian Federation in an international domain.

The geographical location of Russia has been influencing for centuries the way of perceiving the world by the Moscow leadership elites. Starting in the 16th century, they have been forced to pursue their policy in three main directions: The Western one (from the Baltic Sea to theCarpathian Mountains), The Southern one (from the Danube River to Persia) and The Eastern one (from the Volga River to the Altai Mountains).

Keywords: state interest, geographical location, Dugin, geopolitical doctrine.

[*] Polish Internal Security Agency.

[1] Vladimir Markomienko (Russian: ВладимирИгнатьевичМаркоменко) – General Lieutenant, between 1995 and 1996 serving as the I Deputy Director General of the Federal Agency for Government Communication and Information providing support to the President of the Russian Federation (Russian: ФедеральноеагентствоправительственнойсвязиииинформацииприПрезидентеРФ, ФАПСИ). See: А. Колпакиди, *ЭнциклопедиясекретныхслужбРоссии*, Москва 2003, p. 616. Compare: A. Soldatov, I. Borogan, (2010) *The New Nobility. The Restoration of Russia's Security State and the Enduring Legacy of the KGB*, New York, pp. 20, 282, 292.Quoted after: Г. Почепцов, (2000), *Информационные войны. Основы военно-коммуникативных исследований*, Москва, p. 2.

Introduction

Defining the interests of the state in reference to its geographical location is the key element to understanding political actions being taken by the Russian Federation in an international domain. The essence of this reliance is precisely reflected in the views of the orthodox philosopher Nikolai Berdyaev (1874-1947), who coined the statement of "the power of space over the Russian soul". As he wrote, *the Russians do not possess the narrowness of the Europeans, who concentrate their energy on a little space of their souls, neither do they possess the wariness, the economy of time and space, intensity of culture* (Бердяев, 1990, p. 64).The geographical location of Russia has been influencing for centuries the way of perceiving the world by the Moscow leadership elites. Starting in the 16th century, they have been forced to pursue their policy in three main directions:

- The Western one (from the Baltic Sea to the Carpathian Mountains),
- The Southern one (from the Danube River to Persia) and
- The Eastern one (from the Volga River to the Altai Mountains).

That is why they have always tried to stay active in all three areas at the same time, which demands both consolidation of the country and centralization ofitsauthorities (Le Donne, 2004, pp. 15-38; Nowak, 2008, pp. 13-24). Furthermore, existence in the open geographical spaces resulted in constant fear of the outer threat, which implied the tendency to guarantee safety through applying preventive and offensive activities. It is worth underlying that the present foreign policy of Russia shows an increased activity in the following geostrategic areas: from the Balkans, through the Black Sea Basin (Transnistria, Crimea), then through the Caucasus, the Caspian Sea Basin, the whole Central Asia, and then as far as Sakhalin and the Arctic (Gorodetsky, 2003; Grachev, 2005, pp. 255-275; Wiśniewski, 2013, pp. 365-385).

According to some of the Russian elites, the new border layout, being the result of the collapse of the Soviet Russia, is unfavourable when comparing to previous periods. The reflection over geopolitical consequences of that event is still vivid in the minds of representatives of not only the Russian political class, but also the majority of the Russian society. Hence the slogans referring to the reconstruction of the lost empire have been gaining a significant impact on the shape of the foreign policy applied by the Russian Federation, which means that probability of violating international order for geopolitical and geostrategic reasons is relatively high (Grabowski, 2011, pp. 21-22; Кириллов&Крючков, 2008, pp. 10-21). The involvement of Russia in the armed conflicts which took place after 1991 can only confirm that thesis. It is worth underlying that the conflicts were conditioned by, inter alia, geographical locations neighbouring the territories of the post-Soviet areas, especially those with diverse ethnic, social and religious structures, which is particularly meaningful in case of the annexation of Crimea and the events in the West of Ukraine (Grabowski, 2011, p. 38; Эллисон, 2005, pp. 147-191).

Hence it is not surprising that geopolitics in Russia is understood as a political strategy applied also to international relations (Колосов, 1996, p. 86; Колосов &Н.С. Мироненко, 2001, pp. 9-29). What is more, geopolitics in present Russia has gained the status of a general world view, a universal concept which helps to build the world view and one's own attitude towards it (Косолапой, 1996, pp. 57-61; Marciniak, 2004, pp. 4-13; Mäkinen, 2008, pp. 34-49; Isakova, 2005, pp. 10-23). A good example confirming that opinion are the views of ValeryKorovin – the Director of the Centre for Geopolitical Expertise providing support to the Head of the State Duma and a prominent activist for the neo-eurasian movement. His statement published in "Izwiestija" (Russian: «Известия») journal contained precise information about the aims and methods of the Russian policy towards Ukraine, as well as its global context. Valery Korovin distanced himself from the ideological heritage of the Soviet Russia, criticising its leaders for *ideologisation of the foreign policy*. He underlined that *the geopolitical method* applied in order to stop Russia's collapse was recognized as the basis of state security strategy only after Vladimir Putin's rise to power in the Russian Federation. According to Korovin, the basic aim of the Russian foreign policy should be restricting the influence of the "Atlantic Block" (the USA and the European Union) through creating a global, regional and subregional security model. This aim should be achieved by absorbing the countries and the nations belonging in the past to *the Russian space* (close to Russia in civilization and culture) to *theorbit of eurasian geopolitical pole*. According to Korovin, it should be done in the way similar to the annexation of Crimea, which he interpreted as *supporting the regional and local conflicts solving through keeping the peace*. What is more, in Korovin's opinion *the geopolitical method* should be treated as the basis for all actions taken in the Ministry of Defense, the Ministry of Interior and the Federal Security Service, in order to neutralize any threats to security of the state (Коровин, 24 IV 2014; Пустошкин, 1976, pp. 521-522; Grygajtis, 2011, pp. 10-18). The quoted statement reveals that the Russian–Ukrainian conflict is one of the stages in the implementation of the broader political doctrine aiming at strategic reintegration of the post-Soviet space, and in the further perspective – building of the so-called multipolar world. The author of that concept is Aleksandr Dugin – an influential intellectualist and a theoretician of the Russian geopolitics and euroasianism. The basis of the eurasian movement, reborn thanks to Dugin, is a constant thought of rivalry for the power over the space between countries, political-military blocks, international organisations and civilizations (See more Kerr, 1995, pp. 977-988; Smith, 1999, pp. 481-494; O'Loughlin, Toal, Kolossov, 2005, pp. 322-335). Aleksandr Dugin has always claimed that anti-western Eurasian ideology and academic geopolitics serve substantial, far-reaching Russian imperialistic aims. In his opinion geopolitics is: "(…) the worldview of power, education about power and for the power (…). Geopolitics is the discipline of political elites, both the real ones and the alternative ones; its history proves that it is dealt with exclusively by people actively engaged in ruling over nations and countries or preparing to that role (…). In the present world it is the book of power, which should be taken into account while taking global (important) decisions, such as alliances, starting wars, making reforms, restructuring societies, applying economic and political sanctions on a large scale" (Дугин, 1997, pp. 13-14).

The interpretation of the above definition by Dugin shows that geopolitics is a subjective vision of space, rooted in the consciousness of a given society or political environment. It is the result of a rational and subjective calculation of the interests and political goals, as well as cultural factors (historical experience, national myths etc.). Those factors significantly affect the activity of a given subject, which in this particular case is a political practice (Potulski, 2010, pp. 9-10; Tuathail, 1998, pp. 16-39; Lashchenova, 2013, pp. 110-118; Ambrosio, Vandrovec, 2013, pp. 435-466).

According to contemporary researchers, Aleksandr Dugin is a representative of political environments close to the idea of the Russian Empire restoration. This idea became the leading motive of his long political, scientific and journalistic activity. His high position in the narrow circle of the group of people close to President Vladimir Putin is widely known. Dugin officially states that he prepared a lot of geopolitical projects commissioned by the authorities[2]. He is often presented in mass media as an expert or a

[2] А.Г. Дугин, *Стратегические выводы Прямой Линии Путина* [online], http://evrazia.org/article/2505 [availability: 20 VI 2014]: *На теоретическом уровне эта идеология, в центре которой стоит Народ, развита в работе, которую я подготовил по просьбе Кремля ещё в 2007 году, под названием «Обществоведение для граждан Новой России»* (…) *На практическом уровне в 2011 году эта идея – взять Народ в качестве основы идеологии – была как политический проект предложена мной Администрации Президента, в результате чего появился проект Общероссийского Народного Фронта. Я полагал, что эта идеология могла бы стать мировоззренческим ядром «Единой России», но Путин решил иначе.* Compare: В. Иванов, *Дугин – политический Мерлин России* [online], http://www.evrazia.info/article/4377 [availability: 20 VI 2014].

commentator of current political events. An important factor in the biography of Aleksandr Dugin is his relations with high rank representatives of the Russian law and order institutions. It seems obvious that those relations highly influenced his brilliant career. What is more, his initiative has led to creating such political and social organisations as: the International Eurasian Movement (Russian: Международное Евразийское движение, МЕД), the Eurasian Youth Union (Russian: Евразийский союз молодёжи, ЕСМ) and "Izborski Club" (Russian: Изборский клуб). These organisations gather experts from different areas, as well as most noticeable people from the Russian political and cultural world sharing his ideas (Dunlop, 2001, pp. 91-127; Umland, 2010, pp. 144-152; Wojnowski, 2014, pp. 11-38).

The main purpose of this research is presenting the assumptions of the Russian doctrine in relation to Ukraine and specifying the methods of its realisation. First of all, it is necessary to show the relation between Aleksandr Dugin's geopolitical doctrine and some aspects of the Kremlin's foreign policy – both global and regional. This is the subject of the first part of this article. Secondly, it is crucial to define the ways of realisation of foreign policy, which, having in mind Korovin's opinions, may be referred to as "geopolitical method". Basing on his statements it can be said that geopolitical method should be understood as diverse activities helping to achieve a given political doctrine. As it was said before, Korovin suggests that the "geopolitical method" should be mainly applied by law and order institutions. Therefore, a thesis should be advanced here, according to which a "geopolitical method" is also, apart from standard forms of military activities, a wide spectrum of asymmetrical activities. This definition refers to unconventional methods of warfare, such as terrorist activities, information, psychological and economic warfare (Wejkszner, 2009, pp. 120-121; Arreguin-Toft, 2005, pp. 1-48; Katz, 2013, pp. 77-85). The intention of the author of this article is therefore to present the Russian concept of asymmetrical activities, to which one should definitely include the so-called "rebel war" (Russian: мятежевойна) being right now an element of a wide concept of the Russian "information warfare" (Russian: информационная война). A question should be raised to what extent Russia, fulfilling its geopolitical goals in Ukraine, has used the possibilities advanced by such activities. In order to evaluate that, it is necessary to show the analogy between theoretical aspects of such activities and practice, which is the subject of the second part of this article.

The territory of Ukraine in the geopolitical doctrine of Aleksandr Dugin and his supporters

The starting point for considering the meaning of Ukraine in Aleksandr Dugin's geopolitical doctrine is his fundamental masterpiece titled *The Basics of Geopolitics. Geopolitical Future of Russia.* This outstanding book, both in form and content, was released in 1997. It is worth underlying that generals and strategists from the Military Academy of the Russian Federation Armed Forces Headquarters (Russian: Военная академия Генерального штаба Вооружённых сил Российской Федерации) participated in its origin. The book presents geopolitical doctrine, which is supposed to help the rebuilding of the lost empire comparable with the Soviet Russia. Nowadays, this book is the basic position devoted to geopolitics, obligatory in universities and military academies. It gained huge popularity both in Russia and abroad, so it cannot be neglected. The author's ideas are supported by many Russians. What is more, the content of the book constitutes the basis for Dugin's otherwritten works, as well as programs for the political parties and organisations established form his initiative (Dunlop, 2001, pp. 93-94; Eberhardt, 2010, p. 236; Дугин, 2011 și 2012).

The most important task set by Dugin for the Russian nation is the creation of powerful continental empire. The first step on the way to the world's supremacy should be the strategic integration of the post-soviet space and creation of the Eurasian Union, which would be the geopolitical equivalent of the Soviet Russia (Дугин, pp. 170-175; Дугин, 2002, pp. 781-787). One of the basic conditions to reach that goal is, inter alia, spreading the strategic control over the part of the globe described by Dugin as the "Russian South" (Russian: русский Юг), namely the territories located in the northern part of the Balkan Peninsula from Serbia to Bulgaria, Moldova, southern and eastern Ukraine, Rostov, Krasnodar Krai, the Caucasus, eastern and northern coast of the Caspian Sea, the Central Asia (Kazakhstan, Uzbekistan, Kyrgyzstan and Tajikistan) as well as Mongolia, Tibet and Manchuria. Ruling over those territories is just a temporary stage for further expansion to the South and the "warm seas". According to Dugin taking such an action is crucial for securing the Russian borders. In his opinion, leaving those territories in the "geopolitical vacuum" would create a possibility to include them into the "Atlantic" influence zone. The territory of the "Russian South" is treated by Dugin as the main platform of confrontation between the Russian Federation and the "Atlantic" world, the place where the fate of the future empire will be decided of (Дугин, pp. 340-345). However, as he claims, setting the new geopolitical order in this part of the world is not possible without regulating the status of the Ukrainian statehood. In his opinion, taking control over Ukraine would allow Moscow for continuous expansion to the West and to the South. The control over the south-eastern part of Ukraine would assure Russia an inviolable border, which would be the northern coast of the Black Sea. This would restrict the influence of the "Atlantic" Turkey, whose main purpose, according to Dugin, is the realization of the "Turanism-related geopolitical project" – the idea of assembling the Turkish nations, especially the ones living in Kazakhstan, Tatarstan and The Sakha (Yakutia) Republic, which would obviously threaten the Eurasian Union (Дугин, pp. 347–349, 356; Сотниченко, 2011, pp. 4-14; Сотниченко, 2011a, pp. 141-149; Telkin și Williams, 2011, pp. 145-186).

Gaining control over the Western Ukraine would be the first step to decomposing the so-called "dressing station" (Russian: санитарный кордон). This definition, according to Dugin, refers to countries located in the eastern part of a little European peninsula between the Baltic Sea, the Adriatic Sea and the Black Sea. This area has the strategic meaning for the security of the Russian Federation. On one side of this border area the western peripheries of the Eurasian continent are located, on the other side, according to Dugin, there is a bridgehead of the "Atlantic world" subordinate to the Atlantic empire – the USA. Cultural differences multiply geopolitical diversity of that region, since "the dressing station" is the very place of ethnical-religious longitudinal demarcation between the countries of the Latin civilization and the Byzantine Empire heritage (Eberhardt, 2010, pp. 167-187). The "dressing station" include, most of all, Poland, but also Lithuania, Latvia, Estonia, the Western Ukraine, Hungary, Romania, Moldova, the Czech Republic and Slovakia. Dugin underlines that the characteristic feature of foreign policies of the countries located in this region is hostility towards Russia and Germany and servility towards the USA. The existence ofthe "dressing station", which in Dugin's opinion is the product of the Atlantic geopoliticians implemented after World War I, is the source of conflicts between Germany and Russia. What is more, this product prevents the union between the Eurasian Empire and the so-called continental Europe, identified by the geopolitician as being under the German influence. Furthermore, the diversified cultural character of the countries of the "dressing station" hampers their full integration with both the East and the West. That is why it is necessary for Russia to liquidate the "dressing station" through a total reorganization of the Central-Eastern European countries' borders. The new geopolitical order should not be reached through territorial annexation. Instead, Dugin suggests creating several federations of the regions characterized by the uniform geopolitical orientation, which means the ability to integrate in religious, cultural, ethnic and economic aspects with the Eurasian empire or the continental Europe staying under the German control[3]. Taking the religious background under consideration (the dominance of the Catholic and Protestant influences), the Russian geopolitician claims that the following countries stay under the German influence: Poland, Lithuania, Latvia, Estonia, the Czech Republic, Slovakia, Hungary, Romania, Slovenia, Croatia, Bosnia and Herzegovina and the part of Ukraine where Greek-Catholic and strong Ukrainian nationalism dominate. The remaining part of Ukraine should be integrated with the Russian Federation. Other countries of the south-eastern Europe, where the Orthodox Church believers dominate, such as Serbia, Macedonia, Romania, Bulgaria, Moldova, Greece, as well as mostly Muslim Albania should be, in his opinion, included into the Russian influence zone reaching as far as the Ionian Sea (Дугин, pp. 219-228 și 224-226; Бовдунов, 2011, pp. 4-18; Eberhardt, pp. 228-232)[4].

The division of Ukraine, suggested by Dugin, is closely related to the above geopolitical scenario. In his opinion, the existence of Ukraine is unexplainable in the geopolitical sense and its fate is determined by the country's name, which is the synonym of the border region, the buffer zone between the East and the West. He also underlines that no unique civilization has been formed in the territory of Ukraine. According to Dugin, the Dniester River and the Dnieper River, two biggest rivers flowing in the territory of Ukraine, have for ages efficiently restricted the integrative possibilities of this country. He claims that a huge Ukrainian space is inhabited by different "etnos" (Russian: этнос – meaning "society") who have diverse geopolitical goals. The ethnic inhabitants of Great Russia and having the same roots (in

[3] Dugin claims that Belarus, because of Catholic minority with an unfavourable attitude towards the Eurasian Empire, also belongs to the "dressing station". See: А.Г. Дугин, *Основы геополитики…*, pp. 368-370. Compare: Л.В. Савин, *Россия–Украина–Польша: геополитические императивы*, in: *К геополитике*, Л.В. Савин (red.), Москва 2011, pp. 225-235.

[4] It should be underlined that in Dugin's geopolitical arrangement both allied countries, namely Germany and Russia, should cooperate and fight against any aspects of Russophobia in Central Europe and anti-German movements in Russia. Partnership and cooperation of both countries should be confirmed by the project involving liquidation of all mutual agreements and substituting them with tripartite ones – the idea strongly postulated by Dugin. For example, German-Polish or German-Ukrainian, relatively Russian-Polish or Russian-Ukrainian relations and alignments should be changed into agreements of three countries. Russia should become one of the parties in the first case, whereas Germany in the latter one. In result, several countries located between Russia and Germany shall lose any aspects of sovereignty and their future will be decided upon by joined authorities from Moscow and Berlin.

terms of civilization) inhabitants of Little Russia are both Russia-oriented, whereas different in culture "etnos" of the Western Ukraine are becoming a part of the Western-European cultural zone (Дугин, pp. 376-377; Дугин, 2011, pp. 8-25; Багдасарян, 2012, pp. 138-143)[5]. This is why the presently existing Ukraine cannot fully unite with the Eurasian block or the Central Europe, which is under the German influence. In such a geopolitical arrangement, Ukraine – a puppet in the hands of the American politicians – can only exist as a part of the "dressing station", being the source of destabilization of the Eastern Europe and the seed for a potential armed conflict. These are the reasons why a sovereign Ukraine, as it is today, poses a threat to the interests of Russia and is a serious danger to its security, which Dugin identifies with as much as invading the territory of the Russian Federation (Дугин, pp. 347-349; 378-379). That is why, similarly to other countries belonging to the "dressing station", it is necessary to divide Ukraine into four parts of homogeneous geopolitical background, i.e.:

[5]It is worth underlying that Dugin uses the word etnos (Russian: этнос, from the Greek: ethnos) while discussing geopolitical situation of the "dressing station". In his works it means societies strictly bound with the territory they inhabit, possessing a number of special qualities such as: history, language, legislation regulating interpersonal relations, customs and morality. According to his concept, this idea is subordinate to the idea of nation, which is identified with a country and consists of many etnos. See: А.Г. Дугин, *Этносоциология*, Москва 2011, pp. 8-25; В.Э. Багдасарян, *Этнос и проблема цивилизационной идентичности*, w: *Этноцентрум: Сборник материалов по проблемам этносоциологии и социальной антропологии*, А.Г. Дугин, А.Л. Бовдунов (ed.) Москва 2012, pp. 138-143. Hereby Dugin, referring to the theory of Lev Gumilev, creates a scientific legitimization of the process of including different ethnic groups and even national minorities to the "Russian nation". In case of Ukraine, this theory leads to the conclusion that Ukraine is nor inhabited by one Ukrainian nation but individual etnos which leads to the conclusion that Ukraine is not a country and the Ukrainians are not a nation. The Russian geopolitician strongly supported his view in the interview given to the Polish magazine "Fronda" in 1998: "Russians and Germans perceive the world in terms of expansion and we will never change that. We are not interested in just keeping our own country or nation. We are interested in absorbing, by exerting pressure, a maximum number of categories that would complete us. We are not interested in colonization like the British, but in setting our strategic geopolitical borders, even without russification, though some russification sometimes is necessary. In its sacred-geographical evolution Russia is not interested in the existence of independent Poland in any form. Neither Ukraine. And it is not because we dislike the Polish or the Ukrainians – it is because the rights of sacred geography and geopolitics tell so (...) I am convinced that there will be a place for the Germans, the Polish, the French and the Italians in our common Eurasian home. The Russians will only impose the barbarian, sacred lifestyle to the whole Eurasia. The way it works will only depend on a given nation's predispositions. For example, I see the Polish as defenders of the Slavic racism." Quoted after: *Czekam na Iwana Groźnego. Rozmowa z Aleksandrem Duginem. Rozmawiał Grzegorz Górny*,Moscow 1998, „Fronda. Pismo poświęcone" 1998, issue 11-12, pp. 133, 139.

- the Eastern Ukraine, the region on the right bank of the Dnieper River, from Chernihiv to the Sea of Azov, which for ages has been close to Russia in a political, religious and ethnic sense. Dugin does not exclude giving a wide autonomy to that region, but he does not specify its range. In the future, as Dugin claims, that region should be annexed to the Russian Federation,
- the Crimean Peninsula, which should be under the strategic control of Russia. Because of the complex ethnical character of that part of Ukraine, it should be given autonomy taking into account the interests of all "etnos" living there, namely inhabitants of Great Russia, Little Russia and the Crimean Tatars,
- the Central Ukraine spreading from Chernihiv to Odessa (including Kiev). The Central Ukraine is close to the Eastern Ukraine because of the same cultural background and that is why it should be under the Eurasian influence,
- the Western Ukraine, including: Volhynia, Galicia, Transcarpathia and the eastern part of Bessarabia. This part of Ukraine has the main impact on politics in the whole country, being the support for the anti-Russian and pro-Western forces. That is why the purpose of Russia should be not the annexation, but the permanent control over that region through the establishment of the "Western Ukrainian Federation", integrity of which could be regulated depending on the needs. The strategic Russian border should be moved westwards as far as possible (the eastern part of the Central Europe). The cultural-religious border, on the other hand, should be located between the Central Ukraine and the Western Ukraine. Such a solution should help to protect the Orthodox Russia against the influence of Catholicism, as well as the United and Uniting Churches (Дугин, pp. 376-383; Коваленко, 2010, pp. 15-22; Корнев, pp. 25-32; Савин, 2011, pp. 51-64).

In order to eliminate Ukraine as an American policy's tool in the Central-Eastern Europe it is necessary to execute its political decomposition. A successful realisation of that process in the forthcoming years (taking into account that the concept derives from the book published in1997) should be the main imperative of the Russian foreign policy in this part of the world. The Russian Federation cannot become a strategic, political and demographic empire without integration with Belarus and Ukraine (Дугин, pp. 382-383).

The "orange revolution" was the main reason for the radicalisation of Dugin's and his intellectual followers' ideasconcerning Ukraine. The revolution was perceived as artificially planned and supported by the USA with only none aim – to create the government in Kiev whose purpose will be to break off all Ukrainian relations with Russia. That is why the success of the "orange revolution" was treated, for obvious reasons, as a threat to the eurasian empire (Максимов, 2010, pp. 19-23; 27-43; 86-104; Черемных și Восканян, 2013, pp. 60-94; Стариков, 2013, pp. 88-94). It is worth underlying that one of the consequences of that event was setting the concept of not only a close integration of Ukraine with Russia, but also the methods of reaching that goal. For example, stirring an armed uprising in some parts of Ukraine was postulated, which in case of present events has a significant meaning. On 26 April 2006, in the Russian Exhibition Centre, located in the north-eastern administrative part of Moscow, the second convention of the Eurasian Youth Union took place. The society was established by Dugin and it is active both in Russia and in the countries associated within the the Commonwealth of Independent States. During the convention, it was decided that Russia and Ukraine belong to a uniform geopolitical space. It was underlined that the Russian Federation deprived of its relations with Ukraine will lose the status of the Eurasian empire, becoming an Asian country. On the other hand, Ukraine without close connections to Russia is predestined to political and economic marginalization. Pro-Western Ukrainian government, established as a result of the "orange revolution", was recognized as a regime occupying the country. Leonid Savin – the moderator of the Ukrainian fraction of the Eurasian Youth Union, and Valery Korovin – the leader of the organization at that time, who both took part in the convention, postulated establishing the Eurasian Movement and the Eurasian Uprising Army in Ukraine. The basis for that undertaking would be the Eurasian Youth Union, which is active in many Ukrainian cities and regional structures of the National Bolshevik Party (Russian: Национал-большевистская партия, НБП). The main task of the uprising army would be conducting a guerrilla warfare and *getting rid of the invaders in the occupied territory* [6].

[6] Публичная интернет-библиотека Владимира Прибыловского, Съезд ЕСМ объявил повстанческую войну Украине [online], http://www.anticompromat.org/esm/esm02.html [availability: 29 VII 2014]: „Перед членами нового союза выступил координатор ЕСМ Украины Леонид Савин, который пригрозил вновь возрождающемуся оранжевому режиму Украины, что «если оранжевое марионеточное правление на Украине восстановится, то мы начнём сопротивление оранжевой власти, создав Евразийскую повстанческую армию на Украине, а так же евразийский рух» (...) А в условиях, когда Украина захвачена «оранжевой» прозападной марионеточной властью, ЕСМ не видит иных способов очистить оккупированную территорию от захватчиков, кроме как путём создания повстанческого движения – евразийского фронта на Украине. Сегодня ячейки ЕСМ – узлы будущей повстанческой армии находятся во всех городах и населённых пунктах Украины. Как только «оранжевые» вновь объединятся – мы откроем партизанское сопротивление, создав Евразийский Рух и Евразийскую повстанческую армию".

In the following years, Aleksandr Dugin consequently proclaimed his views, treating Ukraine as a deteriorating country suspended in geopolitical vacuum between the West and the East. He also postulated, on numerous occasions, the idea of dividing Ukraine as he suggested in his book *The Basics of Geopolitics*[7]. Interpretation of the events that occurred in Euromaidan led to Dugin reaching for the geopolitical and eschatological-philosophical arguments. In his opinion, the world has been witnessing for ages a planetary struggle between the "Supercivilization of the Sea" (embodied by the USA, the UK, Australia and their allies) and the "Supercivilization of the Land" (embodied by Russia, Continental Europe excluding the UK, the Arabian countries, middle-Asian countries, China, India and Japan). Dugin associates the "Supercivilization of the Sea" with individualism, conformism, materialism,

[7] It is worth to quote some of Dugin's opinions concerning geopolitical future of Ukraine as an example. On 13 August 2008, commenting on the Russian-Ukrainian relationships, Dugin said: "Ukraine acts as if it was a NATO member state, as if its security was guaranteed by a country possessing nuclear weapon. Russia won't accept that. Please, split Ukraine into two parts: Crimea, Kharkov, Donetsk, Kiev will be yours. Volhynia and Ivano-Frankivsk may as well become the NATO members (...) This may end with a war. An armed conflict with Russia about Crimea may lead to a civil war in Ukraine. Who sows the wind, will reap the whirlwind" – quoted after P. Eberhardt, *Koncepcje geopolityczne Aleksandra Dugina*..., p. 236. Compare: A.G. Dugin, *The fate of Ukraine is settled. An interview given to the Russian state television in 2009* [online], http://geopolityka.net/prof-dugin-kwestia-podzialu-ukrainy-jest-juz-przesadzona/ [availability: 29 VII 2014]. In 2013, Aleksandr Dugin formulated three options of solving the problem of Ukraine. The first one assumed the division of Ukraine into two parts: the western and the south-eastern ones. This could prevent a potential civil war, which was to endanger Ukraine. The second option involved a complicated wheeling and dealing with pragmatic Ukrainian authorities in order to make them accept the eurasian integration project under the pressure of circumstances or promises of political, economic and energy advantages. In Dugin's opinion, this would be a peaceful scenario, possible to be implemented in case of a social-economic crisis in Ukraine. In order to reach that goal, one should reach for the "network-centric warfare" arsenal, aiming at subjugating the Ukrainian elites – using both open and clandestine methods – and convincing them to the rightfulness of the Eurasian integration through the use of economic, energy, information and scientific instruments. The third option, according to Dugin the most avant-garde one, assumes the use of the western-Ukrainian nationalists. In his opinion, they do not share the ideas of liberalism, individualism, tolerance, multicultural aspects, human rights and other postmodernist standards, which became dominant in the present western society. Dugin underlines that the Ukrainian nationalism is the main obstacle on the path to the realisation of the eurasian integration project. However, it is worth trying to "convert the poison into the cure" and the enemy into an ally, because the eurasian empire assumes keeping the tradition and the characteristic cultural features of the "etnos" and nations, including the Ukrainian ones. See: А.Г. Дугин, *Евразийскийпроектиегоукраинскаяпроблема* [online], http://www.odnako.org/magazine/material/evraziyskiy-proekt-i-ego-ukrainskaya-problema/ [availabilty: 29 VII 2014]; J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku,* Warsaw 2014, pp. 20–22.

modernism and capital, whereas the "Supercivilization of the Land" with tradition, hierarchy, personalism and collectivism. In mythology, it symbolizes the struggle of Leviathan, i.e. the USA, with Behemoth, i.e. the eurasian civilization (Дугин, 2012, pp. 15-22; Дугин, pp. 14-19, 466-471).

Nowadays, this confrontation takes place both in the ideological and information, as well as in the economic, military and political spheres[8]. The place of the geopolitical rivalry, apart from Transnistria, Caucasus, Abkhazia, the South Ossetia and Georgia, is also Ukraine. According to Dugin, the main goal of the USA is the realisation of the strategy developed by Zbigniew Brzeziński, which assumes separation of Ukraine from the Eurasian civilization, at the same time reducing Russia to the role of a regional superpower. In his opinion, the first step of that strategy execution was the overthrow of the legal authorities in Kiev with the help of Ukrainian nationalists supported by the USA and establishing the anti-Russian government, which started extermination of the Russians living in Ukraine. This is how Russia was made to give a "symmetrical response" to the "Atlantic provocation in Kiev" in the form of the annexation of the Crimean Peninsula, fulfilled with the help of its inhabitants supported by the Russian army. What is more, the Ukrainian crisis being the result of the events in Euromaidan was treated by Dugin as a reason for the revision of Ukrainian integrity. The next step taken in order to "protect the Russian borders" was applying the Crimean

[8] It is worth underlying that cyberspace is also the place of the struggle between the two "supercicilizations". Aleksandr Dugin postulates the development of the Eurasian, multipolar cybergeopolitics based on the use of the Internet. Thanks to that, it will be possible to create virtual, network-centric civilizations that will constitute an opposition block against the Atlantic globalisation, which hostile towards Russia. Virtual civilization should be attached to a given geographical area. They should also possess their own cultural codes, which Dugin understands as paradigm of the activities of numerous, supranational organisations such as religious, political and ecological associations, which thanks to the Internet tools, could effectively promote their ideas. Diverting the vector of the Internet use from a homogenous instrument to a platforms placed in given language systems will cause the rise of the virtual equivalent of the multipolar world. Such virtual platforms, like the Chinese Internet or the Runet, can, in Dugin's opinion, create the basis for a true opposition against the civilization and political monopoly of the USA, which is popularized in the form of globalization. He also claims that the potential of the Internet as a "Global Network" – geopolitical instrument of the West – should be used consciously and with political craftiness in order to reintegrate the post-Soviet space. Dugin suggests creating the project called "Virtual Eurasia" (Russian: ВиртуальнаяЕвразия), whose existence will amount to occupying the broadest possible Internet sector and building its own virtual space. According to him, Eurasia exists not only in the physical, economic and political space, but also in the virtual one. See: А.Г. Дугин, *Попкультураизнакивремени*, Санкт-Петербург 2005, pp. 486–493; B. Gołąbek, *Runet jako extra territorium byłego ZSRR – wokół rosyjskiej cybergeopolityki*, in: *Studia nad rosyjską geopolityką*, L. Sykulski (ed.), Częstochowa 2014, pp. 95-100.

scenario in the eastern parts of Ukraine (Brzezinski, 1997, pp. 30-48; 87-118). It is worth underlying that Aleksandr Dugin, for whom the situation in Ukraine is also a personal matter (his mother was Ukrainian), became actively engaged in the conflict (http://evrazia.org/article/2469). His role in the Russian-Ukrainian confrontation seems to be much broader than just coordination of information, finance and logistic support given to the separatists by his organizations. Aleksandr Dugin is supposed to be one of the authors of the final solution of the Ukrainian problem and the creator of the geopolitical model of the actions taken, which is establishing of the pro-Russian state bodies in the territory of Ukraine. There is evidence for such an assumption. During the Russian-Georgian war he was in the South Ossetia, advising the seizure of Tbilisi and overthrowing of president Mikheil Saakashvili. The next step was to be taking over the Crimean Peninsula, which, as Dugin put it, *is a part of Russia anyway* (Ньюман, [online]). In an interview he admitted that the leaders of the Donetsk People's Republic and the Luhansk People's Republic are his close friends, who in the 90s of the last century took part in his geopolitical courses. He underlined that they took a thorough training and strongly support the idea of neo-eurasianism. He also confirmed that he stays in touch with them. What is more, Dugin claims that the Donetsk People's Republic is the final stage of a political project, which was conceived as a response to the "orange revolution" during a training meeting of the International Eurasian Movement near Volodymyr in 2006[9]. In the context of Dugin's statements, it is worth remembering that in 2006 within the neo-eurasian school of geopolitics and idea of creating the Eurasian Uprising Army in Ukraine was born. Apart from that, he also revealed that his son Artur, a prominent activist of the Eurasian Youth Union, took part in the Crimean operation, as many other activists of the neo-eurasian movement joining the "Crimean Self-Defence". During the operation he performed tasks involving blocking of the Ukrainian government buildings in order to prevent

[9] А.Г. Дугин, *Вводить войска в Новороссию* [online], http://dynacon.ru/content/articles/3314/[availability: 31 VII 2014]: „Да, я многих из них знаю, донецких лидеров практически всех лично, и они действительно мои единомышленники, они патриоты, они с моим участием изучали геополитику, некоторые из них, россияне, вместе со мной ещё с 90-х годов прошли путь патриотической оппозиции. Некоторые из них были в наших лагерях ещё в 2006 году и, кстати, Донецкая республика как виртуальный проект была создана в нашем евразийском лагере под Владимиром в 2006 году. Я нахожусь с ними в постоянном контакте. Таким образом лидеры ДНР и ЛНР, да и всё движение в Новороссии является частью проекта возрождения России, за которую мы многие десятилетия бьёмся, бьюсь я лично, мои соратники по Евразийскому движению, такие, как Александр Проханов и другие. На самом деле в Новороссию вложили своё сердце, душу, всё, что мы имели, все патриоты России, имеющие какое-то влияние".

the leaks of sensitive information (he is also said to have taken part in blocking the Ukrainian party from giving information to the outside world or manipulating the information that was to be given out in the way favourable to the Russian party). Next he decided to become a journalist of Russia Today to take part in the information warfare (Дугин, *Это моя война!* [online]). One of the long-term activists of the Eurasian Youth Union was also Aleksandr Prosiolkov, who until his death on 31 July 2014 was the Deputy Minister of Foreign Affairs of the Donetsk People's Republic (http://rossia3.ru/proselkov3107). It is worth underlying that the main leaders of state administration in the self-appointed republics and their armed forces – Denis Puszylin, Igor Strielkov, Aleksandr Borodaj, Pawel Gubarievand, Valery Bolotov – took part in a special gathering of the "Izborski Club" in Donetsk. It is to be pointed that the organisation itself gathers the most infuential people from the Russian political scene and constitutes an intellectual background for the Kremlin. Aleksandr Prochanov – a writer, politician and the chairman of the "Izborski Club", together with Aleksandr Dugin, Valery Korovin and other experts prepared the project of a new country located in the south-eastern part of "ex-Ukraine". The new geopolitical phenomenon, including the Luhansk People's Republic and the Donetsk People's Republic, was proclaimed on 12 May 2014. This is how a new country, the Federal State of Novorossiya (Russian: Федеративное государство Новороссия, Ukrainian: Федеративна держава Новоросія) was created (http://novorossia.su/ru/node/2386).

The name of the country is not accidental – it is supposed to indicate that the territory in the past belonged to the Russian Empire and the Russian Federation as its successor has the right to annex it (Краснов, 1863)[10]. Dugin underlines that the Donetsk District and the Luhansk District have always been an integral part of Russia and the people living there, who have always

[10] The term „Novorossiya" was used between XVIII and XX century in the Russian Empire and meant the "wild steppe" – the territories located north of the Black Sea and the Azov Sea and south of the borders of the Republic of Poland (before 1793). Nowadays it is the area of the southern part of Ukraine, annexed to Russia in 1774 after the war with Turkey. Between 1764 and 1783 as well as between 1796 and 1802, that territory was the Novorossiya Province divided in 1802 into: Yekaterynoslavska Province, Chersonska Province (1802–1803 – Mikolayovska Province) and Taurydzka Province. Bessarabia (from 1812 a district and from 1873 the Bessarabia Province) and the The Province (Oblast) of the Don Cossack Host (Rostov-on-Don, Taganrog) were also part of Novorossiya. Source: *Россия. Географическое описание Российской Империи по губерниям и областям с географическими картами*, Санкт-Петербург 1913, pp. 58-64. Compare: Н. Краснов, *Материалы для географии и статистики России, собранные офицерами Генерального штаба. Земли Войска Донского*, Санкт-Петербург 1863, pp. 1-596.

been strongly connected to the Orthodox Catholic Church, should be treated as the south-western part of the Eurasian civilization. Those people have always declared their strong connection to Russia. The lands of Novorossiya became a part of Ukraine by accident – in 1991 after the collapse of the Soviet Russia. Those territories may be a part of Ukraine, only when Ukraine integrates with Russia. In Dugin's opinion, the historical identity of the "etnos" from Novorossiya derives from the Russian-Soviet past influenced by Kievan Rus', the Russian Empire, the Orthodox Catholic Church and the Great Patriotic War. According to the authors of Novorossiya, that country is to be subordinate to "sovereign authorities" and free from the influences of the oligarchs, whose wealth should be nationalized (Дугин, *Время Новоросии*; Дугин, *Крым в России. Что дальше?* şi Дугин, *Новороссия часть Русского мира*). Those ideas were also reflected in the political programme of the Social-Political Movement, the Party of Novorossiya (Russian: Общественно-политическое движение «Партия Новороссии»), established on 13 May 2014 by Pawel Gubariev (http://novorossia.su/ru/node/1753).

It should be underlined that some geopolitical concepts proclaimed by Dugin and connected to him the neo-eurasian environment are clearly visible in the Kremlin's activity and president Vladimir Putin's statements. First of all, the key element of the Russian policy towards the new Ukrainian authorities is the demand of the constitutional reforms, which would divert the country from unitary to federal, with a significant privilege of the eastern and southern regions. This can be confirmed by the statement of the Russian Ministry of Foreign Affairs dated 17 March 2014, in which Moscow demanded that the Verkhovna Rada of Ukraine establish a constitutional assembly with the equal representation of all regions belonging to Ukraine. This body would prepare and approve the project of the new constitution. According to the Russian concept Ukraine is to be a "democratic federal state", whose separate regions will have the right to choose independent legislative and executive authorities and will be given broad powers reflecting their historical-cultural specific characters. Extorting such solutions would guarantee Russia the control over the Kiev policy through controlling the policy of the eastern regions of Ukraine. That would mean diverting Ukraine into a lose assembly of federal regions without uniform economic, cultural and social policy and the regions with their legislative authorities would not have to follow the central authorities, which would in particular concern the eastern regions (Olszański, 2014, pp. 1-2; Moshes, 2014, pp. 2-3).

What is more, the president's statements concerning far-reaching geopolitical projects reflect the concept of neo-eurasianism. In one of his statements, Vladimir Putin underlined that Russia is becoming the centre of the

Russian World consisting of the Russian-Ukrainian-Belorussian core. Its main space will consist of the post-Soviet space inhabited by the Russian-speakers. Belonging to the Russian World will be guaranteed by cultural aspects such as language, the Orthodox Church and common values no matter of nationality or ethnic origin (Menkiszak, 2014, pp. 1-7; Panov, 2010, pp. 85-94). Thus, president Putin's views are equal to the definition of Valery Korovin's *eurasian geopolitical pole* being a part of so called multipolar world[11].

[11] After the collapse of the Soviet Russia, the country applied an idealistic vision of creating an international order based on the common interests of all great world powers. In the middle of the 90s of the last century, this idea changed into a realistic vision based on multipolarity. The starting point for that concept became the theory of multipolar world formulated by Aleksandr Dugin. The theory assumes creating a configuration of many centres of power and influence having both contradictory and common interests. See: S. Bieleń, *Erozja monocentryzmu w stosunkach międzynarodowych*, w: *Studia nad geopolityką XX wieku*, P. Eberhardt (ed.), Warszawa 2013, p. 110. Building the eurasian empire, as well as geopolitical reorganization of Europe is a necessary response to the USA's victory in the cold war and the collapse of the Soviet Russia. On the ruins of that communist empire a new, stronger superpower reflecting traditional values of Eastern-Slavic, Turanian and Finn-Ugrian people is to be built. This requires elimination of the unipolar Western World dominated by the power of the USA and substitute it with the bi- or multipolar system. This will enable an expansive policy of the Eurasian empire. The supporters of neo-eurasianism advocate leaving the unipolar world dominated by the USA behind, since in the present world order Russia is no more than a "black whole" placed between the Euro-Atlantic World and the Third World. One of the main goals postulated by the Eurasian policy supporters is mobilization of the resources of the peripheral countries (of the Third World). This in turn is reflected in Dugin's philosophical views, who indicates that postliberalism has blurred the differences between the left and the right. Communism stood against capitalism from the left side and fascism from the right one. He claims that one can stand in the middle, which means accepting the present order, or in the peripheries, which means standing against it. Thus the main Dugin's idea is to mobilize the peripheries, which means mobilizing what has been rejected. In practice, it means metaphysical and political activation of the postindustrial society margins. See: А.Г. Дугин, *Четвертая политическая теория. Россия и политические идеи XXI века*, Санкт-Петербург 2009, pp. 16–17. Next Russia should aim at a close, strategic union with most important European powers (mainly Germany and France). Geopolitical expansion and unions with regional powers such as China, India or Iran shall constitute the basis for consolidation of the potential of the countries belonging to the Eurasian continent. New multipolar world order, in the Eurasian theory supporters' opinion, should be based on creating four main spheres: Anglo-American, Pan-Eurasian, Euro-African and Pacific. The first one would include Anglo-sphere (USA, Canada, the UK, Australia and a part of Polynesia) and the Latin America. The Euro-African sphere would include the European Union and Africa. The areas of the Soviet Russia, Turkey, Iran and India would constitute the Pan-Eurasian sphere, whereas the areas of the East Asia and the South-East Asia would form the Pacific sphere. In further perspective, in the frames of the four mentioned spheres, the neo-eurasian theorists draw a more detailed division: twelve "enormous spheres" as a backward "ideal model" of the future. The twelve spheres include: North-American (USA, Canada, the UK, Australia and a part of Polynesia), Middle-American (the whole continent of the South America), European (the European Union and the European countries associated with the EU: Switzerland, Island and Norway), Arabian-Islamic (the countries of the Maghreb, Sudan the Arabian Peninsula), Transsaharian (the countries of the Transsaharian Africa), Islamic-Continental (mainly Turkey, Iran, Afghanistan and Syria), Indian, Chinese, Japanese and the area of the "new Pacific" (South-Eastern Asia). See: Zob. А.Г. Дугин, *Теориямногополярногомира*, Москва 2013, pp. 276-337; L. Sykulski, *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, in: *Studia nad geopolityką XX wieku*, P. Eberhardt (ed.), Warsaw 2013, pp. 349-365.

Thus, the annexation of Crimea to Russia and the activities of the separatists in the south-eastern part of Ukraine should not be treated as an authentic freedom-related aspiration of its inhabitants described by the Kremlin propaganda as the "Russian Spring". It appeared to be an artificially created geopolitical project implemented with the help of technological social control, as well as information and military aggression. The project was created by the Russian geopoliticians supported by the Kremlin and connected with the eurasian environment identified by Aleksandr Dugin. The true goal, supported by the realization of Dugin's geopolitical doctrine, is most of all a close attachment of the south-eastern areas of Ukraine with Russia, which in the further perspective will deprive the Ukrainian nation of its sovereignty. The real possibility of realizing such a scenario is indicated in the analyses of the main Russian geopoliticians, who draw the vision of the future development of that situation. In that context, a prognosis by Gen. Col. Leonid Iwaszov seems to be particularly interesting. In his opinion, the Euromaidan events started the process of Ukraine collapse. In the perspective of one or two years new referendums – similar to the one that took place in Crimea on 16 March 2014 – are more than probable. Russia should actively support the activities which aim at returning the south-eastern regions to their home country. After "stabilizing" the socio-political situation in those regions, a step further should be taken in the form of a "rebel war" (Russian: мятежевойна).It should affect the western regions of Ukraine, especially where the religious-cultural border goes, which means the line between the Central Ukraine and the Western Ukraine. Thus, it is necessary to provoke strong protests. It can be achieved by the use of, inter alia, disputes on a religious ground, repressive activities of the new authorities and lowering the standard of living of the local inhabitants in comparison with the inhabitants of Novorossiya annexed to the Russian Federation. Thanks to such operations, through the process of the federalization of Ukraine, it will be possible to get the situation "stabilized". Four federal republics would then be established: the Western one with the capital in Lvov, the Central one with the capital in Kiev, the Eastern one with the capital in Kharkiv and the Southern one with the capital in Dnipropetrovsk. According to the general, another scenario is also possible: the mentioned state bodies can be independent, however the economic crisis and the disputes between desiring power and influence oligarchs will lead to a crisis situation. In such circumstances, some "independent countries" may aspire to a close integration with Russia. The Western Ukraine (Lvov) should be deprived of such a possibility. According to Iwaszov, in order to get this idea implemented, strong activity of the Russian institutions and social organizations is necessary. That enigmatic statement should be, of course, understood as the "information warfare" (Ивашов, 2014, p. 11).

Aleksandr Dugin considers a similar scenario for Ukraine. In his opinion, the left part of Ukraine and the regions neighbouring the Black Sea should stay under Russian control. Thanks to that, it will be possible to support the resistance centres against "junta", i.e. the government in Kiev, without the necessity of a direct military intervention (Дугин, *Крым в России. Что дальше?* [online][12]. Valery Korovin also does not consider the existence of Ukraine, as he predicts that it will be split between the Atlantic and Eurasian blocks (Коровин, 2014, pp. 19-21).

The geopolitical plan that Russia has in reference to Ukraine seems to be obvious – it is about a permanent subordination of Ukraine through gaining control over its foreign policy, internal policy, security and economic processes. Thus, keeping an unstable situation in Donbass is just an instrument applied in order to keep control over the whole Ukraine.

Evgeny Messner's "rebel war" as an element of the Russian "information warfare" on the example of the Russian-Ukrainian conflict

According to Gen. Leonid Iwaszov, the main method of the realization of the Russian geopolitical goals in the territory of Ukraine is the so-called "rebel war". Theoretical basics of that phenomenon were described by Colonel of the General Headquarters of the Tsarist Army and veteran of both world wars, who spent the last years of his life as a scientist of military academies in Argentina – Evgeny Messner (1891-1974).

As early as in the 60s of the last century, he warned the world against the era of unconventional wars, today referred to as asymmetrical or irregular[13]. Messner's scientific interests concerned psychological aspects of the art of war, soldiers' and officers' morale and different forms of conflicts[14].

[12] А.Г. Дугин, *КрымвРоссии. Чтодальше?*[online], http://dynacon.ru/content/articles/2864/ [availability: 31 VII 2014]: *Вся территория Украины вряд ли будет дружественной России, точка не возвратапройдена. Поэтому задача теперь запереть хунту в Правобережье (граница – русло Днепра, а на Юге к России отходит вся полоса Причерноморья – это необходимо, чтобы прервать черноморско-балтийский санитарный кордон). Параллельно естественному кошмару, который начнётся на Правобережье, в этой Киевской-галицкой державе, можно будет поддержать очаги сопротивления хунте и на Западе, но на сей раз точно без прямого участия войск*.

[13] Compare footnote 16 of this article.

[14]Е.Э. Месснер, *Ликсовременнойвойны*, in: *Военнаямысльвизгнании. Творчество русской военной эмиграции*, И.В. Домнин (ed.), Москва 1999, pp. 363-404. DetailedbiographyofEvgenyMessnercanbefoundin: И.В. Домнин, *От Первой мировой до «Третьей Всемирной». Жизненный путь Генерального штаба полковника Е.Э. Месснера*, w: *Хочешь мира, победи мятежевойну! Творческое наследие Е.Э. Месснера*, И.В. Домнин (ed.), Москва 2005, pp. 18-51; К. Александров, *Армия генерала Власова 1944-1945*, Москва 2006, pp. 26, 41-42, 182, 248, 507; И.В. Домнин, *Краткий очерк военной мысли Русского Зарубежья*, in: *Военная мысль в изгнании. Творчество русской военной эмиграции*, И.В. Домнин (ed.), Москва 1999, pp. 448-527.

Basing on his personal experience and erudite knowledge supported by knowledge of a few foreign languages, Messner published numerous monographs, articles and research, among which special attention should be paid to *World Rebel War* (Russian: *Всемирная Мятежевойна*) published in Buenos Aires in 1971. Its integral part constitutes a study titled "Mutiny, or the name of the Third World War" (Russian: *Мятеж – имя Третьей Всемирной*) published in 1960 in the capital of Argentina as a separate study[15].

Revolution in Russia, philosophy of the Sun Tzu art of war, both world wars and numerous regional conflicts are said to be the inspirations of Evgeny Messner's search for the genesis of a new way of waging war. Taking precise observation, Messner concluded that regular soldiers' fight is often entwined with riots of political, social and economic backgrounds or with terror attacks and activities carried by secret organizations, sabotage groups and individuals. These activities are difficult to classify. It is also hard to point to their origin. He called the new phenomenon "fighting with a rebellion" (Russian: борба мятежом), shortly "rebel war" (мятежевойна, from Russian мятеж – rebellion, riots). In Messner's opinion, psychological aspect was barely used in the past wars, but in "rebel war" it is to be the main tool. That is why "rebel war" is to be the psychological warfare. Messner underlines that in the future, this will be the prevailing way of waging wars and his abovementioned study is just an exiguous one, not covering the whole problem[16].

The main rule of waging a "rebel war" is using national movements, rebellion etc. as the subjects of revolution (Месснер, 2004, pp. 15-23, 332-340). According to Messner, revolution is most of all a psychological

[15] Neither Polish nor Western researches have recognised Evgeny Messner's academic works. It is worth remembering that his leading monographs have not been translated into English so far. A scientist who has recently took an interest in that issue in our country is Kazimierz Kraj. See: K. Kraj, *Wojny asymetryczne czy miatieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku*, „Bezpieczeństwo. Teoria i praktyka" 2012, issue 3, pp. 33-41; idem, *Мятежевойна Jewgienija Messnera*, "E-Terroryzm" 2012, issue 2, pp. 16-18.

[16] It should be noted that waging wars using asymmetrical activities was the subject of deep study of the Nazi philosopher Carl Schmitt. In one of his works, he suggested that such activities should be legally legitimized in international law. See: C. Schmitt, *Theorie des Partisanen Zwischenbemerkung zum Begriff des Politischen*, Berlin 1975; T. Kochi, *The Partisan: Carl Schmitt and Terrorism*, "Law Critique" 2006, issue 17, pp. 267-295. Schmitt's views became the basis of Dugin's statements, who claims that guerilla groups using terrorist methods of fight constitute the main tool in the conflict between the "Supercivilization of the Sea" and the "Supercivilization of the Land" and Russia, because of its traditions of the Napoleonic Wars and the Great Patriotic War, is an *enormous guerrilla empire.* Dugin's opinions are thus a trial (though only ideological one for the time being) to legitimize the asymmetrical activities applied in the Russian policy. See: А.Г. Дугин, *Философия войны*, Москва 2004, pp. 96-100.

phenomenon, which should be understood as a quick and radical change in people's consciousness. The art of revolution is based on creating and separating an active group led by revolutionary leaders from the society or a nation. Revolution is characterized by psychological processes taking place in masses stimulated by active groups. It bases on law instincts and psychology of the masses, as result of which a civilized man becomes a barbarian. According to Messner's concept, psychology of the "rebellious masses" is the main tool leading to victory or failure. The aim of a war is not only neutralization of the enemy's armed forces, but also destabilization of the whole country with the use of psychological factors: demoralization, fear and the feeling of uncertainty being the result of guerrilla and terrorist groups activities (Schmid, 2005, pp. 137-146). That is why a "rebel war" is often described by Messner as a "half-war", which should be understood as a transitional stage between peace and conventional war activities. "Rebel war" is also characterized by the impossibility of precise determination of the conflict parts, hidden behind and carrying out activities using irregular "non-state" groups (Месснер, 2004, pp. 46–59). It is also hard to point the exact starting point and the end of such a war, in case of which there are no such terms as theatre of war or the front line in their standard meaning. The main goal of a "rebel war" – according to Messner – is *gaining control over the enemy's soul*. That is why in order to be successful it is necessary to make a psychological profile of not only people, but most of all the whole group, society or nation. That implies huge challenges for the new form of intelligence – the so-called psychological intelligence (Russian: психоразведка) (Месснер, 2004, pp. 105-116). Activities are carried out not only in traditional space (land, sea, air), but also (most of all, in fact) in the human psyche. The concept of the front line in case of a "rebel war" refers to individual spheres of society's activities such as economy, politics, culture etc. An important goal of a "rebel war" is the process of your own nation's integration and winning a part of the enemy's nation over to your side. That is the task for journalists, saboteurs, provocateurs and propagandists. All social groups of the enemy should be put under psychological pressure. According to Messner, an important role in that activity have political parties and social organizations. The secret of keeping psychological control over the rebelled masses is based on defining their needs and shaping their new consciousness (neo-consciousness) in a way that they treat as expressing their own will (Месснер, 2004, pp. 59-64; Зелинский, 2008; Кириллов, 2012, pp. 71-74).

After general description of genesis, definition and aims of a "rebel war", Messner presents its main participants. He divides them into four groups:

1. "rebel masses" (Russian: мятежные массы) meaning disobedient citizens or revolting crowds, constituting the biggest in number and the most disorganised group taking part in a conflict. This group is characterized by unpredictability and radicalism of attitude passing from activity to passivity and vice versa, which is a big challenge for the operational command, in traditional art of war comparable to commanding coalition troops.
2. "rebel columns" (Russian: мятежные колонны), described also as "cryptoarmy" or "secret police", meaning individuals or groups chosen from the "rebel masses" whose main tasks concern terrorist and subversive activities. Members of such groups can be described as ideologists serving the idea they fight for. "Rebel columns" are mainly saboteurs, terrorists and provocateurs.
3. "rebel militia" (Russian: мятежное ополчение) meaning irregular, voluntary guerrilla groups or insurgent army. This group is strictly bound to the nation or ethnic group it comes from. "Rebel militia" is territorial, which means it stays active in the area its members come from and is usually supported by local population.
4. "army in a rebel war" (Russian: войско в мятежевойне), which constitutes an equally important element during a conflict. Activities of "rebel masses", "rebel columns" and guerrilla groups should be coordinated with the task of a regular army. In Messner's concept regular army plays only a supportive role to guerrilla groups, "citizen militia", revolting social groups or national minorities (Месснер, 2004, pp. 65-73; Beckett, 2001; Arquilla, 2012; Larson, Eaton, Nichiporuk, Szayna, 2008; Svete, 2009, pp. 381-399).

Cooperation of the four abovementioned groups should aim at reaching precisely defined goals, which Messner defined as:

- disintegration of the hostile nation's morale;
- disintegration of active parts of the country (army, guerrilla groups, social movements);
- taking over or deactivating objects of psychological value;
- taking over or deactivating objects of material value;
- implementing activities aiming at winning allies or weakening the enemy's allies;

- protection of your own nation's morale;
- saving your own armed forces;
- securing your own objects of psychological and material value,
- neutralising the factors that could potentially lead to neutral countries' reaction (it should be taken into consideration that not only governments, but also social groups may react) (Месснер, 2004, pp. 110–116 and 212).

It should be mentioned that Evgeny Messner's concept of a "rebel war" was reflected in the early 90s of the last century, during the creation of the Russian asymmetrical activities doctrine, incorporated in the broad concept of "information warfare". The operation in Crimea and escalation of the Russian-Ukrainian conflict gave the possibility to evaluate the concept of Russian "information warfare", which became the subject of a thorough study by Jolanta Darczewska (2014). She acknowledged that the Russian theorists understand the concept of information warfare as influencing the consciousness of the masses in the international rivalry of the civilisation systems in the information space, which can be achieved by the use of special ways of control over information resources, used as "information weapon". The Russian concept of "information warfare" refers to psychological warfare and specpropaganda used during the times of the Soviet Russia. The author underlined that the technological dimension of information warfare in Russia has been marginalized and pushed out from the public space, at the same time giving place to cultural and ideological factors. The main task of "information warfare" is reaching precise aims in foreign, regional and internal policy, as well as securing geopolitical advantage. Nowadays, in Russia there are two schools of "information warfare" established by Igor Panarin and Aleksandr Dugin – the main representatives of the concept of geopolitics and leaders of the public opinion, having connection with special services. The author claims that they try to sensitise their own society to information threats from the outside, at the same time formulating the Russian system of information counteracting. They deal with the concept of "information warfare" both in theory and in practice (Месснер, 2004, pp. 11-18).

It is worth pointing to numerous studies by Igor Panarin, Aleksandr Dugin, Valery Korovin or Leonid Savin, which have popularizing, disinformation and propaganda function, discussing in detail mainly the American concept of information warfare. Its aim, as the authors claim, is disintegration of Russia and destabilization of the post-Soviet space. They also point to the alleged weakness of Russia and the necessity to build their own concept of "information warfare" in order to oppose the aggression from the

West, which previously caused the Soviet Union collapse (Дугин, 2007, pp. 321-347; Савин, 2011; Савин, 2012; Коровин, 2014, pp. 177-309; Коровин, 2009; Панарин, 2010). Comparing studies of the abovementioned authors with theses of the American theorists lead to the conclusion that the definitions and methods of implementation of "information warfare", allegedly Russian, have been taken from the American works (not far from the abovementioned definitions) and have been adjusted to the Russian propaganda purposes. This could be confirmed by Dugin's journalistic activity, in which he recognized the American concept of waging Network Centric Warfare and being its integral part the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) formula as main tools of stirring "flower revolutions" in the post-Soviet territories. Basing on the American literature he created the model of "Eurasian network", which is supposed to be a response to the American "Network Centric Warfare challenge" (Дугин, pp. 333-347; Дугин, 2008, pp. 2-10; Дугин, 2013, pp. 38-68; Ferris, 2004, pp. 199-225; Kipp, 2014, p. 36; Бедрицкий, 2008, pp. 54-86). A similar concept was also formulated by Igor Panarin, who adopted the American theory called noopolitik into the Russian grounds (Панарин, 2006, pp. 163-172; Arquilla, Ronfeldt, 1999).

Thus, the concept of "information warfare" by the abovementioned authors, which is strictly related to the American original, is hard to be recognized as a real reflection of the practice applied in the Russian Federation. It is then worth to ask a question about the authentic theoretical assumptions of the Russian information warfare and its realization. While analyzing this problem, it is also worth to pay attention to the achievements of the army in the subject matter. Theoretical and practical aspects of this kind of war have been studied by the armed forces of the Russian Federation from the beginning of the 90s of the last century. These activities were stimulated by the American achievements in the area of operations conducted on the basis of information during the war in the Persian Gulf, no matter how close they were to Evgeny Messner's concept of a rebel war based on the information-sociological factors (Grau, Thomas, 1996, pp. 508-511; Thomas, 1996-1997, pp. 81-91; Heickerö, 2010, pp. 13-15; Лебедев, Лютов, Назаренко, 1991, p. 14).

Definitions of "rebel war" formulated by the Russian servicemen are quite universal and refer to activities conducted both during wartime and peacetime. It is to be pointed that they are not to be found in the studied by geopoliticians, political scientists and leaders of the public opinion. In the military nomenclature, the term "information warfare" is not used. In Russia it is reserved for publicists, scientists and civil analysts. In the military environment, the terms “information confrontation” (Russian: информационное противоборство) or “information fight” (Russian: информационная борьба) are preferred. Both terms are used interchangeably and the difference between them is not clear enough (Grau, Thomas, pp. 516-517; Воронцова, Фролов, 2006, pp. 3-5). It is then worth to mention a few chosen definition as examples. In the 90s of the last century, one of the pioneer theoreticians of this form of conflicts, Col. Sergey Komov, defined information warfare as information counteracting, as well as protection of your own sources with the use information according to a uniform plan aimed at winning and keeping advantage over your enemy. He claims that should be just one of many diverse actions taken against your enemy (Комов, 1996, pp. 76-80; Комов, 1994, pp. 16-17; Комов, 1997, pp. 18-22). Anonymous officer of the Military Academy of the Russian Federation Armed Forces Headquarters, quoted by Timothy Loyd Thomas, comes up with a similar definition of information confrontation. In his opinion, it is just one of many forms of resolving conflicts between the parties, whose goal is to win and keep information advantage over your opponent. This can be achieved by applying information-technical and information-psychological means, through affecting the decision-makers, command and control system, people and information sources of a given country (Thomas, 2003, pp. 208-210; Clogg, 1997, pp. 425-430).

The opinion of Vladimir Cymbal – an analyst in the Russian Ministry of Defence, who considers the definition of information warfare in both broad and narrow senses, is equally meaningful. In his opinion, information warfare in the broad sense is a set of activities applied by one country against the citizens of another country or group of countries during peacetime. These activities concern the influence on the society’s consciousness through education, art, culture, education system, administration etc., which should be carried out by civil special services – the Federal Security Service and the Foreign Intelligence Service. The latter one’s main task should be getting control over the information sources of other countries, sabotage of information technologies development in the countries treated as hostile and neutralizing communication systems and information networks of the enemy. An important task of that service is also building and implementing the systems guaranteeing the information security of Russia. On the other hand, “information warfare” in the narrow sense means military activities aiming at getting information advantage over the enemy in the scope of information spreading, use and processing, as well as implementing effective decisions allowing for getting advantage in the battlefield. The realization of this sphere of information warfare should be the responsibility of the Ministry of Defence and the armed forces[17].

The definitions presented here imply that the Russian "information warfare" is a set of diverse, coordinated in time activities, carried out by both military forces and civil special services in many areas, in order to neutralize the enemy with the use of information-technological and information-psychological tools. An American Col. Timothy Loyd Thomas, dealing with the subject matter for two decades, has tried to classify those activities. Basing on an extensive material confronted with the statements (which he knew from his own experience) of representatives of the Russian military environment, taking part in conferences in Washington and Moscow as long ago as in 1996, he created a precise structure of the Russian "information warfare", radically different from the one promoted by the Russian military technologists. According to T. L. Thomas, the Russian "information warfare" is characterized by a diversity of means and flexibility of activities in many distant spheres, which is valid even today. It takes the following elements:

- philosophical aspect of "information warfare";
- information security as an aspect of national and global security;
- information sources as government potential;
- the definition of information warfare.
- computerization of armed conflicts:
    - electronic tools of armed conflicts;
    - automation of armed conflicts;
    - application of robots in armed conflicts;

[17] T.L. Thomas, *The Russian View of Information War*,in: *The Russian Armed Forces at Dawn of the Millennium 7-9 February 2000*, M.H. Crutcher (ed.), Carlisle 2000, pp. 338, 342-343; S. Blank, *Russian Information Warfare as Domestic Counterinsurgency*, „American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy" 2013, issue 35, no. 1, p. 41; K. Giles, *"Information Troops" – a Russian Cyber Command?*, w: *Third International Conference on Cyber Conflict*, C. Czosseck, E. Tyugu, T. Wingfield (ed.), Tallinn 2011, pp. 45–60. It should be underlined that the first of the definitions given by V. Cymbal refers to the Russian concept of the "ideological sabotage" or "ideological rebellion". See: *Контрразведывательныйсловарь*, Москва 1972, pp. 90–91. A lot of information concerning the "ideological sabotage" was revealed by the KGB officer and correspondent of RIA Novosti Jurij Bezmienow, vel Thomas Schuman. In his opinion, the "ideological sabotage", which he associated with psychological warfare, ideological aggression and propaganda warfare, is a long-term process (lasting for the last 15-25 years) divided into four stages: "Demoralization", "Destabilization", "Crisis" and "Normalization". The goal of that process is to subjugate a given country without the need for starting an open armed conflict. See: T.D. Schuman (J. Bezmienov), *Love Letter to America*, Los Angeles 1984, pp. 17-46. Compare: idem, *No "Novosti" is Good News*, Los Angeles 1985; idem, *World Thought Police*, Los Angeles 1986.

  - intellectual tools of armed conflicts (intelligent weapon allowing for precise strikes);
- fight computerization (operation preparation);
- battlefield computerization (battlefield digitalization).
- information-psychological warfare:
  - military-patriotic education of your homeland citizens;
  - moral-psychological preparation of the military staff;
  - psychological operations against civilians and military staff of the hostile country.
- information-technical warfare:
  - applying communication and control systems in a confrontation;
  - the role and place of intelligence in information warfare.
  - the use of special programmes aiming at:
    1) destroying information source;
    2) redistribution of information sources;
    3) protection of information sources.
- preparation of the personnel meant to take part in information warfare,
- aspects of the international law concerning information warfare (Thomas, 1996, p. 34; Thomas, 1998, pp. 40-62; Thomas, 2009, pp. 465-491).

It should be mentioned that in the beginning of the 90s of the last century, a net structure consisting of civil special services (FAPSI, FSB, SWZ) and a part of the armed forces was created. It was responsible for information warfare and perfecting its methods, which include both psychological and technical elements (Thomas, 1998, pp. 156-172). They refer to the Russian pattern of the "ideological sabotage" and Evgeny Messner's concept of "rebel war". Thus, it should be concluded that promoting the image of the Russian Federation as a victim of the aggression form the West and a country completely unprepared to face "information warfare" is just disinformation aiming at justifying the "war against «information warfare» carried out against Russia". The Russian concept of "information warfare" is evolving and is constantly adjusted to a current geopolitical situation (Thomas, 2010, pp. 265-301; Goble, 2009, pp. 181-196). It could be confirmed by deliberations of two distinguished theoreticians associated with the Centre of War-Strategic Studies of the Russian Federation Armed Forces Headquarters (Russian: Центр военно-стратегических исследований Генерального штаба Вооружённых Сил Российской Федерации): Col. Sergey Czekinov and (retired) Gen. Lt. Sergey Bogdanov (Main, 2000, pp. 47-62; Чекинов, 2010 pp. 3-5; Giles, 2014, p. 21). They have applied the term "asymmetrical activities" (Russian: асимметричные действия) into the Russian grounds defining it as complex and systematic activities of political, diplomatic, economic, information and military character. They show that the information confrontation should play an important role in the process of a given country's management system and control disorganization. It should also influence public opinion, resulting e.g. in anti-government demonstrations and destabilization of a given country or other entity being the target of those operations, whose essence is to be the use of intellectual advantage. In that context, operating with the systems of presenting the world, the people, the essence of civilisation and directions of its development, as well as the most important values, should be recognized as the contemporary "information warfare" (Russian: информационное оружие).

Apart from the information-technical and information-psychological factors, scientific-technical and political-psychological instruments should also be used. These technologies help to influence the subjects of "information warfare". The main goal of that type of war is to manipulate the consciousness of a society or a nation with false visions of the surrounding world and thus directing and stimulating their activities. The subject of information confrontation is then the system of traditional values, ideals and myths constituting the basis of a given nation's culture and its self-identification. The ultimate goal is making the victim to accept the aggression and treating the imposed way of thinking and actions as their own. That is why geopolitics is so important in case of "information warfare", since it provides scientific argumentation serving as a weapon in waging this type of war. On the other hand, the meaning of asymmetrical activities in the military sphere should be reaching the goal without an armed struggle. This is to be reached through intimidating the enemy and making him realize, by demonstrating the military readiness in a strategic territory or destroying his most dangerous entities, that a potential armed struggle is useless (Чекинов și Богданов, 2010, pp. 13-22; Thomas, 2014, pp. 105-106; Короход, 2013, p. 302; Бухарин, Цыганов și Бочкарева, 2013, pp. 14-21; Цыганов, Васин, Бухарин, 2007, pp. 25-30; Бухарин, Матвиенко, 2008, pp. 2-9; Rothstein, 2007, pp. 160-187; Лайнбарджер, 2013).

The events taking currently place in Ukraine are a model example of the use of theoretical aspects of the Russian asymmetrical activities presented above. It is then worth to study every single stage of the conflict in comparison with the theory. On 28 February 2014, an operation was launched in Crimea, aiming at taking the military control over the peninsula by Russia. The operation was participated by the local troops of "Crimean Self-Defence", supported by unidentified formations of the Russian army. They took control over most of the strategic facilities such as airports, communication junctions and passages, as well as the buildings belonging to the Ukrainian army and the Security Service of Ukraine. Within a week, the whole peninsula was under control. Though some buildings stayed under the Ukrainian army control, they were blocked and deprived of any ability to conduct military activities through cutting off energy, water and other supplies. The most significant fact is that the whole operation was conducted without an open fight between the parties of the conflict. Self-appointed authorities from Simferopol started forming the autonomous armed forces on the basis of the local self-defence troops and the buildings taken away from the Ukrainian army. Armed soldiers with hidden faces wearing uniforms without any emblems, called "green people" or "gentle people" surprised the world media and analysts ironically commenting the conflict. They took over the airport in Sevastopol claiming that they had come to defend it against the "Bandera troops from Kiev". However, they did not inform anyone who they were and what country they come from. When it was clear that the alleged troops did not pose any threat to the airport, they were withdrawn. At the very moment the information was publicized, they came back and took the airport over again[18].

These activities are evident enough to be referred to as the so-called psychological special operations (Russian: психологические специальные операции) being within the competence of special operations troops GRU. One of that formation's ex-members, Col. Vladimir Kvaczkov explains that their goal is to manipulate people's (both servicemen and civilians) consciousness and emotions, by means of confusion and demoralization, in order to make them feel friendly towards the Russian army (Квачков, 2010, p. 376). This was reached by removing all the emblems from the soldiers' uniforms, making it unable to identify the country (so-called crypto-operation) and the formation they serve for, as well as by forbidding to communicate, in any form, with the civilians. All this led to many

[18] Because of the information warfare going on in both Russian and Ukrainian media, the primary source allowing for the reconstruction of actual events of the conflict are the analyses prepared by the experts of the Centre for Eastern Studies in Warsaw. See: A. Wilk, *Rosyjska interwencja wojskowa na Krymie* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [availability: 16 VIII 2014]; T. Iwański, W. Rodkiewicz, A. Wierzbowska-Miazga, A. Wilk, *Rosja wobec Ukrainy: nie tylko Krym* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-12/rosja-wobec-ukrainy-nie-tylko-krym [availability: 16 VIII 2014].

contradictory interpretations of “green people”, “soldiers in uniforms” or “gentle people” and inability to define the enemy and taking the right actions. What is more, the effect of surprise was achieved, which allowed Russia for its own interpretations of events: during the peaceful demonstration in Maidan, over one hundred people died, whereas during the military intervention in Crimea no one was hurt. This operation was also described as *strategic provocative information n-driven operation* (Russian: стратегическая наступательная информационная операция) aimed at preceding the military intervention with preparations based on the use of information (Почепцов, *Информационные операции и Крым: базовые причины для манипуляций* și *Информационные операции и Крым: причины и следствия. Часть 2* [online])[19]. Thus, the Russian activities in Crimea confirm one of the rules of a “rebel war” – the one concerning the use of rebelling masses put over the years under the adequate psychological-information pressure (so-called intoxication) (Darczewska, 2014, p. 20; Nord, 2004, pp. 87-111) supported by regular army. To reach that goal, multidirectional and mass activities were initiated: federal TV and radio channels, newspapers and the Internet sources. This was supported by diplomats, politicians, political scientists, experts, as well as the elites of science and culture. The arguments were given that the real threat to Crimea comes from the “Bandera troops invading the peninsula”, “the NATO troops taking control over the Black Sea Fleet” or “derussification of the Ukrainian citizens”. It was also said that the government in Kiev was established by foreign special services, especially American and Polish ones, whose espionage network (being the property of the Military Information Services, WSI) had been for years the tool of the American interests in Ukraine, especially in the petrol-energetic sector (Савин, 2008, pp. 50-51). As it was mentioned before, participation of activists from the Eurasian Youth Union in the Crimean operation was also confirmed, which complies with the definition of the “rebel columns”. As Evgeny Messner predicted, the army was played a secondary role. The first line belonged to the “rebel masses” and the “rebel columns” taking over individual buildings and facilities. The goals were reached by the information-psychological pressure, sabotage and economic sanctions, without any armed struggle, taking over an intact infrastructure and avoiding casualties among soldiers and activists, as well as among the inhabitants of the peninsula. An important element was also

[19] For regulations concerning the international law on wearing uniforms and emblems during armed conflicts see: W. Hays Parks, *Special Forces’ Wear of Non-Standard Uniform*, w: *International Law Studies. Issues in International Law and Military Operations*, J.B. Jaques (ed.), Newport 2006, pp. 69-121.

president Vladimir Putin's attitude, who stayed calm and misinformed the western leaders (Cimbala, 2014, pp. 359-379; Berzins, 2014, pp. 1-7; Darczewska, pp. 5-6; 31-32; Vázquez Liñán, 2009, pp. 137-159).

The Crimean scenario was repeated in the next months. On 6 April 2014 in Donetsk, Kharkiv and Luhansk, groups consisting of several hundred to two thousand pro-Russian activists rebelled, which ended with taking over government buildings. In Kharkiv and Donetsk, local government buildings and the buildings of SBU were also taken over. The activists made similar political demands, which confirms that the action had been planned before and it was coordinated by and consequently directed from Russia. On the Eurasian Youth Union's website one could find the instructions on "self-organization" and taking buildings over by crowds (*Молот Правды. Жителям Юго – Востока: инструкция по самоорганизации* [online]). The establishment of the Donetsk People's Republic and the Kharkiv People's Republic were proclaimed and in Luhansk people refused obedience to the government of Ukraine. On 11 May 2014 a referendum on sovereignty of the Donetsk and Luhansk Districts was organized. On 12 May 2014, a resolution on the Luhansk People's Republic and the Donetsk People's Republic sovereignty was passed and negotiations on establishing Novorossiya were started. This was a breaking moment and passing to another stage of the conflict, when the authorities of the self-appointed republics established armed militia with an important role of instructors from Russia (Iwański, Menkiszak, *Prorosyjski "separatyzm" narzędziem przymuszenia Ukrainy do federalizacji* [online:]).

The example of Igor Strielkov vel Girkin is quite significant in that context. On 15 April 2014, the SBU Press Service announced that one of the leaders of the subversive group of separatists occupying government buildings in Sloviansk was indentified. It appeared to be the abovementioned Igor Strielkov who, according to the SBU, was a soldier of the GRU Spetsnaz, which made it obvious that the separatists were instructed and supported by the Russian military intelligence. Strielkov soon became the subject of information warfare between the parties of the conflict: Ukraine exposed his connections to the Russian special services in order to prove the engagement of those services in the separatist activities, whereas the Russian propaganda made Strielkov a hero of national fight for freedom. Thus a historian and historical re-enactments enthusiast was to become a soldier in the fight for the freedom of Novorossiya – voluntarily, as a patriot (Скоморохов, 20.V.2014). Strielkov himself admits that he has never been a member of the GRU, but the FSB. His real name is Girkin and "Strielkov" is his false name (Виноградов, 5.VII.2014).

Aleksandr Czerkasov, the President of the Foundation of Human Rights "Memoriał", exposed interesting details concerning true activities of Igor Girkin. Basing on relations of the witnesses, he revealed that in 2001 Girkin participated in murders and kidnapping of the Chechen citizens, at that time serving for the 45 Independent Regiment for Special Operations of the

Airborne of the Russian Federation Armed Forces (Russian: 45-й Отдельный полк специального назначения Воздушно-десантных войск Вооружённых Сил Российской Федерации) (Черкасов, May 21, 2014). The main task of the military formations of that type was special intelligence (Russian: специальная разведка) with all available means – from observation, through combat actions aiming at the seizure of the demanded persons or facilities, to radio-technical intelligence (Министерство обороны РФ, *Разведывательная Подготовка Подразделений ВДВ*, pp. 5-10, 56-71).

An important part of their activity is also *special operations concerning formation, support and combat use of irregular forces* (Russian: специальные операции по формированию, поддержке и боевому применению иррегулярных сил). According to Kvaczkov, such operations aim at establishing irregular formations performing the tasks of armed forces, which Russia is vividly interested in. They include intelligence tasks for the guerrilla groups and insurgent troops, as well as for the organizations involved or likely to get involved in a given conflict. It also includes any kind of help, especially in the area of training and logistics, as well as the use of numerous means of operational protection with the help of the espionage network available (Квачков, 2010, p. 376). So it can be concluded that the example of Strielkov is a vivid confirmation of the Russian support for the Luhansk and Donetsk militia and separatists, both during preparations and during the conflict itself. The SBU accused Strielkov of directing the operational activities in Crimea, aiming at preparation of the invasion and liquidation of the Ukrainian espionage network in Sloviansk and Kramatorsk (Скоморохов, 20.V.2014). It should however be underlined that the front line of armed activities belongs to the militia, the Russian special forces playing a supportive role. An interesting example of that is a telegram from Strielkov in which he reports that his personal source of information from Kiev informed him about an attempt of making a reportage by the Ukrainian TV station. The reportage was to be about “the alleged crimes of the Russian soldiers”. Next Strielkov asks Dugin to publicize that information on the Internet, fact which is supposed to give the Russians advance and discredit the Ukrainian attempt (*Сводки от Стрелкова Игоря Ивановича. Сообщение от ополчения* [online]). So here we have a vivid example of providing the separatists with information support by the Russian special forces. The militia consists of several-people groups carrying out guerrilla activities. Their leaders come from the military environment, very often from Russia or having been trained in that country. It should be considered that they had precise knowledge about the theatre of armed activities and its character, since many veterans of special forces serving in Ukraine left to Russia after the collapse of the Soviet Russia (Козлов, 2010, pp. 151-161). After starting an open fire with the Ukrainian army those troops very often withdrew trying to drag them into the street fight. They also organized traps which were very effective. A good example and confirmation of that could be the operation carried out on 22 May 2014 under the town of Wolnovacha, in which separatists shattered the 55 Mechanical Brigade of the Ukrainian Armed Forces killing 18 and injuring 32 soldiers, which was the biggest loss for the Ukrainian army in its 23-year history. The separatists were supported by civilians who blocked the Ukrainian columns. So here we have a clear example of cooperation between "rebel masses" and "rebel militia" described by Evgeny Messner (Żochowski, Wilk, şi Konończuk, *Konflikt w Donbasie – wymuszona deeskalacja?* [online]).

Equally important element of a "rebel war" is activating the "rebel columns". The definition that Messner came up with may be referred to the groups of mercenaries and volunteers not only from Russia, but from the whole post-Soviet territory and even from the Balkans. It is widely known that among the "Novorossiya defenders" there is a Serbian troop of about 250 people called "Jowan Szewicz". The ascending number of mercenaries is accompanied by the delivery of military equipment and any other supplies from the territory of the Russian Federation.

It appears that supported by Moscow mercenaries took control over local separatists groups[20].

Russian activities in the territory of Ukraine revealed the effectiveness of organizations of a new kind. One vivid example can be the Eurasian Youth Union, whose activists evidently supported separatists by organizing referenda in Moscow and ensuring information support, but most of all by

[20] Aleskandr Matjuszyn, nickname "Warjag", one of the leaders of the Donetsk People's Republic's armed forces, can be an excellent example of ideological attitude characterized by Messner in his definition of "rebel columns". He gave an interview in which he revealed the backstage of his activities in Ukraine, where his main goal was to prepare an uprising. After graduating from university, he started his political activity in the ranks of the Moscow skinheads, taking part in riots and street fights. Next, he joined Dugin's National Bolshevik Party (NBP) LED by Eduard Limonov. After returning from Moscow he dealt with establishing the party structures in the Donetsk district. However, he left the party after "Limonov's selling himself to the liberals". During the "orange revolution" he was one of the founders of the campaign called "Ukraine without Yushchenko". After leaving the party he joined a new movement called the Donetsk Republic (Russian: движение «ДонецкаяРеспублика»). He directed its activities in the town of Makiejevka. He got arrested by the SBU. Since he dealt with training the youth groups of the Donetsk Republic, in 2007 he was accused of leading illegal armed troops. Aleskandr Matjuszyn underlines a huge role of his cooperation with Dugin's Eurasian movement supporters and the Russian nationalists at that time. He said that the establishment of the Donetsk People's Republic was not accidental – it was a long-time plan of the activists. His statements make it clear that they were supported by Moscow. After declaring the independence of the Donetsk People's Republic he was appointed as the commander of the Volunteer Battalion "Warjag" (Russian: Добровольческийбатальон «Варяг»), subordinated to the Ministry of State Security of that republic. The main goal of that battalion, apart from the front fight, is also fighting and getting rid of "saboteurs" and "thieves". M. Учитель, *Александр «Варяг» Матюшин: нам нужна республика нового типа* [online], http://rossia3.ru/politics/vatjag_matyushi [availability: 31 VII 2014].

coordinating humanitarian help (Публичная интернет-библиотека Владимира Прибыловского, *Евразийский Союз Молодежи* [online]). On 14 May 2014, on the organization's official website one could spot an announcement about the recruitment to *the volunteer squads fighting the Nazi American mercenaries and oligarchs in the territory of Novorossiya* (Евразийский Союз Молодёжи, *Помощь Донбассу, записаться добровольцем!* [online]). Pavel Karnishev, the present leader of the organization, informed that a group of about one thousand volunteers was formed. Paramilitary organization called the Eurasian Youth Union is a youth fraction of International Eurasian Movement. The Eurasian Youth Union was established during the convention that took place on 26 January 2005 in which about 600 participants took part. The present number of its members is unknown. The union's structures are active not only in Russia, but also in other countries belonging to the Commonwealth of Independent States, as well as in Germany, Italy and Romania. Its strict leadership include Pavel Karnishev, Dmitri Jefremov, Arthur Dugin and Aleksey Bielajev-Gintovt– the oganization's "stylist". The union has military-like organized structures, both centrally and locally (Публичная интернет-библиотека Владимира Прибыловского, *Евразийский Союз Молодежи*…).

The main leaders are called moderators. The idealistic profile of the union is characterized by radical anti-American attitude and the hostile attitude towards the West. However, the idealistic profile created by Aleksandr Dugin is also shaped by the occult references[21]. The main goal of the union is to establish Eurasian army and carry out Eurasian revolution. The Eurasian Youth Union has a network structure; it tries to influence the widely understood youth environment, using the arsenal characteristic for information warfare. The most important role here has the Information-Analytical Division, the so-called information cell of the KGB, which was directed by Valery Korovin (Публичная интернет-библиотека Владимира

[21] It is Worth mentioning that the emblem of the Eurasian Youth Union is a stylized "Chaos Star", the symbol of magical rebirth in the West. The symbol, taken by Dugin from the works of an occultist Aleister Crowley, refers to the "magic of chaos". Since for Dugin the term "chaos" is a synonym of a different, opposite to the western culture term "order", creating new possibilities of action and reaching political goals. Dugin had a positive attitude towards Crowley's works (who, by the way, was an MI-6 agent) and wrote that *radical revolutionary trends were perceived by Crawley as the realization of the equinox storm with the help of the powers of chaos in order to wipe out the remains of the rotten civilizations, getting closer to the logical and cyclical end.* See: L. Sykulski, *Koncepcja Radykalnego Podmiotu i „czwarta teoria polityczna" Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejskiej*, „Przegląd Geopolityczny" 2014, issue 8, p. 236; A.G. Dugin, *The Multipolar World and the Postmodern*, „Journal of Eurasian Affairs" 2014, issue 2, pp. 11-12.

Прибыловского, *Коровин Валерий Михайлович* [online]; *Катехизис члена Евразийского Союза Молодежи* [online]; Arquilla, Ronfeldt, 2001, pp. 1-25). Without any doubts that organization is an information support to the Kremlin. Its members deal with information warfare in a scientific dimension. In 2007 the union's activists carried out a cyber-attack on the Ukrainian president's website. After that incident, the Ukrainian structures of the organization were strictly controlled by the SBU, which led to many of its members leaving the union (*Евразийские боевики из Восточного Казахстана?* [online]).

It is however worth underlying that the Eurasian Youth Union is only one of many "rebel columns". Aleksandr Dugin and his supporters very quickly adopted the idea of "information warfare". Its concept was borrowed by Dugin from the ideologists of the so-called New Right movement. Getting political power (in the region, country or the whole continent) should be accompanied by imposing one's culture, the way of thinking and the system of values. In order to reach that, one should carry out a cultural-ideological invigilation of university environments and representatives of such professions as doctors or lawyers, who influence the public opinion. Such an idea was postulated by Alain de Benoist, who is widely respected among the eurasianists and strongly supports the "Fourth Political Theory" by Aleksandr Dugin. The Eurasian Youth Union is just a part of a bigger organization of a network character, which is a "conveyor belt" of ideology coming directly from Moscow[22].

Conclusions

To sum up, it should be underlined that Russia has presented its own concept of "information warfare" to the hole world. In this particular case we can talk about diversification and synchronization of many activities. Their common feature is the use of information and its processing as the main weapon based on the psychological factors supported by the use of modern technological solutions. Information warfare takes asymmetrical activities, which are skilfully directed. All the factors mentioned above create a unique, Russian concept of "hybrid warfare", which constitutes a serious threat for the security of the widely understood West. The Russian way of carrying out a conflict, in its far genealogy, refers to the Sun Tzu war philosophy and the military heritage of the people from the East, based on the concept of the

[22] An example of the network is another organization called the Global Revolutionary Alliance, GRA, established by Dugin. This is a new type organization not officially bound to the centre it works for. Such organizations realize the so-called strategy of non-directed resistance. See: L. Sykulski, *Koncepcja Radykalnego Podmiotu…*, p. 238. Compare: J. Tomasiewicz, *Strategia oporu niekierowanego w wojnie asymetrycznej*, „Przegląd Geopolityczny" 2009, issue 1, pp. 161-191.

maximum weakening of the enemy at the expense of the minimum own losses. Taking into account the specifications of the Russian activities and possible scenarios of the situation development, one should consider that in case of Kiev's disagreement to the federalization of the country the war, irrespective of its form, may last for years. It is probable that the divisions between the parties of the civil war, because of so many victims, will deepen and the constant "occupation" of the eastern districts by the government forces will be inevitable in order to stabilize that part of Ukraine. The occupation, on the other hand, will mean spending money on huge military bases equipped with the latest military technology and the maximum operational protection of that region by the Ukrainian special services, which may be very costly for that country. In further perspective, this situation may lead to escalation of the conflict, carried out not only in the form of regular fight, but also typically terrorist activities in the territory of the whole country, making it unstable. The situation may be compared to Ulster[23].

The difference is that the Ukrainian case is much larger in scale. The world media reports about terrorist attacks in Ukraine will be equally natural as the ones reporting another bomb explosion in Iraq or Palestine. However, there is one possible scenario. The separatists will be given support (both human and technological) allowing them not only to keep Donbas, but also to carry out offensive activities further into the western part of the country. The potential for such activities is significant: in Odessa, Kharkiv, Zaporizhia or Dnipropetrovsk thousands of separatists are waiting for orders and weapon. The economic crisis and the rise of anti-government movements in Ukraine may only be in favour of such scenario. A different matter are the separatist movements in the Zakarpattia Oblast, which are said to escalate along with the internal problems form the neighbouring Moldova. In this case the official military intervention from Russia should also be considered as one of the possibilities.

[23] The conflict in Ulster (Northern Ireland) is the most known and described European conflict, in which terrorist methods were used. The main reasons of that conflict was the desire of the Irish nationalists and Republicans (mainly Catholics) the province governed by the UK to the Republic of Ireland. This was opposed the Unionists (mainly Protestants) who claimed their integrity with the UK. The conflict took both military and political basis, with simultaneous engagement of politicians, paramilitary and terrorist organizations, as well as the UK and Irish security forces. The activities were carried out mainly in the territory of the Northern Ireland. From time to time, they escalated to the territories of England, Ireland and the continental Europe. It lasted until the end of the 60s of the last century, until the signature of the Good Friday Agreement in Belfast in 1998. Regardless of the agreement occasional attacks till take place. See: J. Loughlin, *The Ulster Question Since1945*, London–New York 2003; J. Muller, *Language and Conflict in Northern Ireland and Canada: A Silent War*, London–New York 2010; L.A. Smithey, *Unionists, Loyalists, and Conflict Transformation in Northern Ireland*, Oxford 2011.

References:

1. Dugin, A.G., (March 14, 2014), *Geopolityka znaczenia. Semantyczna wojna wokół Ukrainy* accesibil pe http://xportal.pl/?p=13003.
2. Бердяев, Н.А., (1990), *Судьба России. Опыты по психологии войны и национальности. Репринтное воспроизведение издания 1918 г.*, Москва 1990.
3. Le Donne, J.P., (2004), *The Grand Strategy of the Russian Empire, 1650–1831*, Oxford.
4. Nowak, A., (2008), *History and Geopolitics. A Contest of Eastern Europe*, Warsaw.
5. *Russia between East and West: Russian Foreign Policy on the Threshold of the Twenty-First Century,* (2003), G. Gorodetsky (ed.), London.
6. Grachev, A., (2005), *Putin's Foreign Policy Choices,* w: *Leading Russia: Putin in Perspective Essays in Honour of Archie Brown,* A. Pravda (ed.), Oxford.
7. Wiśniewski, R., (2013), *Przemiany terytorialne państwa rosyjskiego – aspekt historyczno-polityczny,* in: *Studia nad geopolityką XX wieku,* P. Eberhardt (ed.), Warszawa.
8. Grabowski, T.W., (2011), *Rosyjska siła. Siły Zbrojne i główne problemy polityki obronnej Federacji Rosyjskiej w latach 1991–2010,* Częstochowa.
9. Кириллов, В.В., Крючков, Ю.Н., (2008), *Влияние войны на развитие и международное значение России в мире,* în "Военная мысль", issue 2.
10. Р. Эллисон, (2005), *Россия, региональные конфликты и применение военной силы*, in: *Вооруженные силы России: власть и политика*, С.Э. Миллер, Д. Тренин (red.), Кембридж–Лондон.
11. Колосов, В.А., (1996), *Российская геополитика: традиционные концепции и современные вызовы*, "Общественные науки и современность", issue 3.
12. Колосов, В.А., Мироненко, Н.С., (2001), *Геополитика и политическая география: Учебник для вузов*, Москва.
13. Косолапой, Н.А., (1996), *Геополитика как теория и диагноз (метаморфозы геополитики в России)*, "Бизнес и Политика", isuue 4, pp. 57–61;
14. Marciniak, W., (2004), *Przestrzeń jako kategoria dyskursu politycznego w Rosji współczesnej*, Warsaw.
15. Mäkinen, S., (2008), *Russian Geopolitical Visions and Argumentation. Parties of Power, Democratic and Communist Opposition on Chechnia and NATO, 1994–2003*, Tampere.
16. Isakova, I., (2005), *Russian Governance in 21th Century. Geostrategy, Geopolitics and Governance*, London–New York.
17. Ištok, R., Plavčanová, D., (2013) *Russian Geopolitics and Geopolitics of Russia. Phenomenon of Space*, "European Journal of Geopolitics", issue 1.
18. Sykulski, L. (2014), *Geneza rosyjskiej geopolityki*, w: *Studia nad rosyjską geopolityką*, L. Sykulski (ed.), Częstochowa.
19. Коровин, В., (April 24, 2014), *Геополитика вместо идеологии*, "Известия"[online], http://izvestia.ru/news/569829 [availability: 20 VI 2014].

20. Пустошкин, В.В., (1976), *Геополитические теории войны*, in: *Советская военная энциклопедия. Том 2: Вавилон – Гражданская война в Северной Америке*, А.А. Гречко (red.), Москва.
21. Grygajtis, K., (2011), *Józef Stalin oraz sowiecka geopolityka i geostrategia lat 1924–1953*, Nysa.
22. Kerr, D., (1995), *The New Eurasianism: The Rise of Geopolitics in Russia's Foreign Policy*, "Europe-Asia Studies", issue 47.
23. Smith, G., (1999) *The Masks of Proteus: Russia, Geopolitical Shift and the New Eurasianism*, "Transactions of the Institute of British Geographers. New Series", issue 24.
24. O'Loughlin, J., Toal, G., Kolossov, V., (2005), *Russian Geopolitical Culture and Public Opinion: The Masks of Proteus Revisited*, "Transactions of the Institute of British Geographers. New Series", issue 30.
25. Дугин, А.Г., (1997) *Основы геополитики. Геополитическое будущее России*, Москва.
26. Potulski, (2010), *Współczesne kierunki rosyjskiej myśli geopolitycznej: między nauką, ideologicznym dyskursem a praktyką*, Gdańsk.
27. Tuathail, G.Ó., (1998), *Postmodern Geopolitics? The Modern Geopolitical Imagination and Beyond*, w: *Rethinking Geopolitics*, Ó Tuathail, S. Dalby (ed.), London–New York.
28. Lashchenova, E. (2013), *National Archetypes of Russia's Foreign Policy*, "International Affairs. A Russian Journal of World Politics, Diplomacy and International Relations" 2013, issue 2.
29. T. Ambrosio, G. Vandrovec, (2013), *Mapping the Geopolitics of the Russian Federation: The Federal Assembly Addresses of Putin and Medvedev*, "Geopolitics", issue 18, no. 2.
30. Г. Дугин, *Стратегические выводы Прямой Линии Путина* [online], http://evrazia.org/article/2505 [availability: 20 VI 2014].
31. В. Иванов, *Дугин – политический Мерлин России* [online], http://www.evrazia.info/article/4377 [availability: 20 VI 2014].
32. J.B. Dunlop, (2001), *Aleksandr Dugin's "Neo-Eurasian" Textbook and Dmitrii Trenin's Ambivalent Response*, "Harvard Ukrainian Studies", issue 25.
33. A. Umland, (2010), *Aleksandr Dugin's Transformation from a Lunatic Fringe Figure into a Mainstream Political Publicist, 1980–1998: A Case Study in the Rise of Late and Post-Soviet Russian Fascism*, "Journal of Eurasian Studies", issue 1.
34. M. Wojnowski, (2014), *Aleksandr Dugin a resorty siłowe Federacji Rosyjskiej. Przyczynek do badań nad wykorzystaniem geopolityki przez cywilne i wojskowe służby specjalne we współczesnej Rosji*, "Przegląd Bezpieczeństwa Wewnętrznego", issue 10.
35. A. Wejkszner, (2009), *Wojny XXI wieku. Istota współczesnych konfliktów asymetrycznych*, in: *Zagrożenia asymetryczne współczesnego świata*, S. Wojciechowski, R. Fiedler (ed.), Poznań.
36. I. Arreguin-Toft, (2005), *How the Weak Win Wars: A Theory of Asymmetric Conflict*, Cambridge.
37. D.J. Katz, (2013), *Waging Financial War*, "Parameters", issue 43, pp. 77-85.

38. P. Eberhardt, (2010), *Koncepcje geopolityczne Aleksandra Dugina*, “Przegląd Geograficzny”, issue 82.
39. А.Г. Дугин, (2011), *Геополитика: Учебное пособие для вузов*, Москва.
40. А.Г. Дугин*, (*2012*), Геополитика России: Учебное пособие для вузов*, Москва.
41. *Политсовет ОПОД «Евразия», Евразия превыше всего (манифест Евразийского движения)*, in: *Евразийский взгляд. Основные принципы доктирнальной евразийской платформы*, Н. Мелентьева (ed.), Москва 2001.
42. А.Г. Дугин, *Россия может быть или великой, или никакой*, in: *Основы евразийства*, А.Г. Дугин (ed.), Москва 2002.
43. А.Г. Дугин, *Основы геополитики…*
44. А.А. Сотниченко, *Турция: геополитическая ось Евразии*, in: *Геополитика. Информационно-аналитическое издание. Выпуск IX: Турция*, Л.В. Савин (ed.), Москва 2011.
45. А.А. Сотниченко, *Геополитика Турции*, w: *Левиафан: Материалы семинаров по проблемам геополитики и многополярности*, А.Г. Дугин (ed.), Москва 2011.
46. A. Telkin, P.A. Williams, *Geo-Politics of the Euro-Asia Energy Nexus. The European Union, Russia and Turkey*, London 2011.
47. P. Eberhardt, *Koncepcja granicy między cywilizacją zachodniego chrześcijaństwa a bizantyńską na kontynencie europejskim*, “Przegląd Geograficzny” 2010, issue 76.
48. А.Г. Дугин, *Основы геополитики…*, pp. 368-370. Compare: Л.В. Савин, *Россия–Украина–Польша: геополитические императивы*, in: *К геополитике*, Л.В. Савин (red.), Москва 2011.
49. А.Л. Бовдунов, *Политико-географические образы Центральной и Восточной Европы и геополитическая организация региона*, in: *Геополитика. Информационно-аналитическое издание. Выпуск X: Восточная Европа*, Л.В. Савин (ed.), Москва 2011.
50. А.Г. Дугин, *Этносоциология*, Москва 2011, pp. 8-25; В.Э. Багдасарян, *Этнос и проблема цивилизационной идентичности*, w: *Этноцентрум: Сборник материалов по проблемам этносоциологии и социальной антропологии*, А.Г. Дугин, А.Л. Бовдунов (ed.) Москва 2012.
51. *Czekam na Iwana Groźnego. Rozmowa z Aleksandrem Duginem. Rozmawiał Grzegorz Górny,*Moscow 1998, “Fronda. Pismo poświęcone” 1998, issue 11–12.
52. А.А. Коваленко, *Перспективы федерализации Украины*, w: *Геополитика. Информационно-аналитическое издание. Выпуск II: Украина*, Л.В. Савин (ed.), Москва 2010.
53. А.Ю. Корнев, *Государственно-правовые аспекты развития крымского регионализма*, w: *Геополитика. Информационно-аналитическое издание…*,pp. 25-32; Л.В. Савин, *Национально-политическая идентификация в Украине и формы репрезентации власти*, w: *К геополитике*, Л.В. Савин (ed.), Москва 2011.
54. И.В. Максимов, *Цветная революция-социальный процесс или сетевая технология?* Москва 2010.

55. К. Черемных, М. Восканян, *Анонимная война*, "Изборский клуб" 2013, issue 6.
56. Н. Стариков, "*Оранжевая кровь*", "Изборский клуб" 2013, issue 10.
57. Публичная интернет-библиотека Владимира Прибыловского, Съезд ЕСМ объявил повстанческую войну Украине [online], http://www.anticompromat.org/esm/esm02.html [availability: 29 VII 2014]:
58. A.G. Dugin, *The fate of Ukraine is settled. An interview given to the Russian state television in 2009* [online], http://geopolityka.net/prof-dugin-kwestia-podzialu-ukrainy-jest-juz-przesadzona/ [availability: 29 VII 2014].
59. А.Г. Дугин, *Евразийский проект и его украинская проблема* [online], http://www.odnako.org/magazine/material/. evraziyskiy-proekt-i-ego-ukrainskaya-problema/ [availabilty: 29 VII 2014];
60. J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku,* Warsaw 2014.
61. А.Г. Дугин, *Геостратегический контекст противоборства морских и континентальных держав*, in: *Геополитика. Информационно-аналитическое издание*. *Выпуск XIV: Евразийский Союз*, Л.В. Савин (ed.), Москва 2012.
62. А.Г. Дугин, *Попкультура и знаки времени,* Санкт-Петербург 2005, pp. 486–493; B. Gołąbek, *Runet jako extra territorium byłego ZSRR – wokół rosyjskiej cybergeopolityki,* in: *Studia nad rosyjską geopolityką,* L. Sykulski (ed.), Częstochowa 2014.
63. А.Г. Дугин, *О Новороссии и вводе войск. Геополитический анализ* [online], http://novorossia.su/ru/node/3321 [availability: 29 VII 2014].
64. Группа экспертов во главе с Сергеем Глазьевым, *Украина: между Западом и Россией*, "Изборский клуб" 2014, issue 4.
65. Z. Brzezinski, *The Grand Chessboard. American Primacy and Its Geostrategic Imperatives*, New York 1997.
66. А.Г. Дугин, *Украинцев я очень люблю, я сам – украинец* [online], http://evrazia.org/article/2469, [availability: 29 VII 2014].
67. Д. Ньюман, *Кто придумал аннексировать украинский Крым? Многие россияне симпатизирует новому виду милитаристского патриотизма авторства Александра Дугина* [online], http://evrazia.info/article/4839 [availability: 31 VII 2014].
68. А.Г. Дугин, *Вводить войска в Новороссию* [online], http://dynacon.ru/content/articles/3314/ [availability: 31 VII 2014].
69. А.Г. Дугин, *Это моя война!* [online], http://dynacon.ru/ content/articles/3274/ [availability: 31 VII 2014].
70. А.Г. Дугин, *В Крыму надо ввести духовную цензуру...* [online], http://crimea.mk.ru/articles/2014/06/04/aleksandr-dugin-v-krymu-nado-vvesti-dukhovnuyu-cenzuru.html [availability: 31 VII 2014].
71. Евразийский союз молодёжи, *Убит лидер ЕСМ по ЮФО Александр Просёлков* [online], http://rossia3.ru/proselkov3107 [availability: 31 VII 2014].
72. *Александр Проханов разработает идеологию Новоросии* [online], http://novorossia.su/ru/node/2386, [availability: 31 VII 2014].
73. *В Донецке состоялось первое заседание филиала Изборского клуба – Новороссия,* http://novorossia.su/ru/node/2783 [availability: 31 VII 2014].

74. *Идеология Новороссии. Изборцы предлагают своё видение идейной основы для нарождающегося на юго-западных рубежах РФ государства*, "Изборский клуб" 2014, issue 5.
75. *Россия. Географическое описание Российской Империи по губерниям и областям с географическими картами*, Санкт-Петербург 1913, pp. 58–64.
76. Н. Краснов, *Материалы для географии и статистики России, собранные офицерами Генерального штаба. Земли Войска Донского*, Санкт-Петербург 1863.
77. А.Г. Дугин, *Время Новоросии* [online], http://dynacon.ru/content/articles/3309/ [availability: 31 VII 2014].
78. *Крым в России. Что дальше?* [online], http://dynacon.ru/content/articles/2864/ [availability: 31 VII 2014];
79. *Новороссия часть Русского мира* [online], http://dynacon.ru/content/articles/3419/ [availability: 31 VII 2014].
80. *Программа Общественно-политического движения "Партия Новороссии"* [online], http://novorossia.su/ru/node/1753 [availability: 31 VII 2014].
81. T.A. Olszański, *Ukraina: suwerenna decentralizacja czy niesuwerenny federalizm*?, "Komentarze OSW" 2014, issue 134.
82. A. Moshes, *More Stick, Less Carrot: Russia's Policy Towards Ukraine Following Recent Events*, "Russian Analytical Digest" 2014, issue 146, pp. 2–3.
83. M. Menkiszak, *Doktryna Putina: Tworzenie koncepcyjnych podstaw rosyjskiej dominacji na obszarze postradzieckim*, "Komentarze OSW" 2014, issue 131.
84. P. Panov, *Nation-building in Post-Soviet Russia: What Kind of Nationalism is Produced by the Kremlin?* "Journal of Eurasian Studies" 2010, issue 1.
85. S. Bieleń, *Erozja monocentryzmu w stosunkach międzynarodowych*, w: *Studia nad geopolityką XX wieku*, P. Eberhardt (ed.), Warszawa 2013.
86. А.Г. Дугин, *Четвертая политическая теория. Россия и политические идеи XXI века*, Санкт-Петербург 2009.
87. Zob. А.Г. Дугин, *Теория многополярного мира*, Москва 2013, pp. 276–337;
88. L. Sykulski, *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, in: *Studia nad geopolityką XX wieku*, P. Eberhardt (ed.), Warsaw 2013.
89. Л.Г. Ивашов, *Будущее Украины и Россия*, "Изборский клуб" 2014, issue 5, p. 11.
90. А.Г. Дугин, *Крым в России. Что дальше?* [online], http://dynacon.ru/content/articles/2864/ [availability: 31 VII 2014]:
91. В. Коровин, *Гибель Украины*, "Изборский клуб" 2014, issue 5.
92. Е.Э. Месснер, *Лик современной войны*, în: *Военная мысль в изгнании. Творчество русской военной эмиграции*, И.В. Домнин (ed.), Москва 1999.
93. K. Kraj, *Wojny asymetryczne czy miatieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku,* "Bezpieczeństwo. Teoria i praktyka" 2012, issue 3.
94. idem, *Мятежевойна Jewgienija Messnera*, "E-Terroryzm" 2012, issue 2.
95. C. Schmitt, *Theorie des Partisanen Zwischenbemerkung zum Begriff des Politischen*, Berlin 1975.

96. T. Kochi, *The Partisan: Carl Schmitt and Terrorism*, "Law Critique" 2006, issue 17, pp. 267–295. А.Г. Дугин, *Философия войны*, Москва 2004, pp. 96–100.
97. Е.Э. Месснер, *Всемирная мятежевойна*, Москва 2004, pp. 15–23, 332–340.
98. A. Schmid, *Terrorism as Psychological Warfare*, "Democracy and Security" 2005, issue 1..
99. С.А. Зелинский, *Информационно-психологическое воздействие на массовое сознание. Средства массовой коммуникации, информации и пропаганды — как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс*, Санкт-Петербург 2008.
100. А.В. Кириллов, *Информационно-психологическое воздействие на массовое сознание посредством СМИ (на примере операций по информационному обеспечению «MISO» военных конфликтов начала XXI в.)*, "Армия и общество" 2012, issue 2.
101. I.F. Beckett, *Modern Insurgencies and Counter-Insurgencies: Guerrillas and Their Opponents since 1750*, London–New York 2001.
102. J. Arquilla, *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World*, Lanham 2011.
103. M. Kennard, *Irregular Army: How the US Military Recruited Neo-Nazis, Gang Members, and Criminals to Fight the War on Terror*, New York 2012.
104. E.V. Larson, D. Eaton, B. Nichiporuk, T.S. Szayna, *Assessing Irregular Warfare. A Framework for Intelligence Analysis*, Santa Monica 2008.
105. U. Svete, *Asymmetrical Warfare and Modern Digital Media: An Old Concept Changed by New Technology?* w: *The Moral Dimension of Asymmetrical Warfare, Counter-terrorism, Democratic Values and Military Ethics*, Th.A. van Baarda, D.E.M. Verweij (ed.), Leiden–Boston 2009.
106. А.Г. Дугин, *Геополитика постмодерна. Времена новых империй. Очерки геополитики XXI века*, Санкт-Петербург 2007.
107. Л.В. Савин, *Сетецентричная и сетевая война. Введение в концепцию*, Москва 2011.
108. idem, *От шерифа до террориста. Очерки о геополитике США*, Москва 2012; В.М. Коровин, *Третья мировая сетевая война*, Санкт-Петербург 2014.
109. *Главная военная тайна США. Сетевые войны*, Москва 2009; И.Н. Панарин, *Первая мировая информационная война. Развал СССР*, Санкт-Петербург 2010.
110. А.Г. Дугин, *Теоретические основы сетевых войн*, "Информационные войны" 2008, issue 1.
111. *Сетевые войны (аналитический доклад)*, "Изборский клуб" 2013, issue 10.
112. J. Ferris, *Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?* "Intelligence and National Security" 2004, issue 19.
113. J.W. Kipp, *'Smart' Defense From New Threats: Future War From a Russian Perspective. Back to the Future After the War on Terror*, "Journal of Slavic Military Studies" 2014, issue 27.
114. А.В. Бедрицкий, *Информационная война: концепции и их реализация в США*, Москва 2008.

115. И.Н. Панарин, *Информационная война и геополитика*, Москва 2006.
116. J. Arquilla, D.R. Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica 1999.
117. L.W. Grau, T.L. Thomas, *A Russian View of Future War: Theory and Direction*, "The Journal of Slavic Military Studies" 1996, isuue 9.
118. T.L. Thomas, *Deterring Information Warfare: A New Strategic Challenge*, "Parameters" 1996–1997, issue 26.
119. R. Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Stockholm 2010.
120. Ю.В Лебедев, И.С. Лютов, В.А. Назаренко, *Война в зоне Персидского залива: уроки и выводы*, "Военная мысль" 1991, issue 11–12, p. 14.
121. Л.В. Воронцова, Д.Б. Фролов, *История и современность информационного противоборства*, Москва 2006.
122. С.А. Комов, *Информационная борьба в современной войне: вопросы теории*, "Военная мысль" 1996, issue 3.
123. idem, *О концепции информационной безопасности страны*, "Военная мысль" 1994, issue 4, pp. 16–17; idem, *О способах и формах ведения информационной борьбы*, "Военная мысль" 1997, issue 4.
124. T.L. Thomas, *Information Warfare in the Second (1999–) Chechen War: Motivator for Military Reform?*, in: *Russian Military Reform 1992–2002*, A.C. Aldis, R.N. Mc Dermott (ed.), London–Portland 2003.
125. R. Clogg, *Disinformation in Chechnya: An Anatomy of a Deception*, "Central Asian Survey" 1997, issue 16.
126. T.L. Thomas, *The Russian View of Information War*,in: *The Russian Armed Forces at Dawn of the Millennium 7–9 February 2000*, M.H. Crutcher (ed.), Carlisle 2000.
127. S. Blank, *Russian Information Warfare as Domestic Counterinsurgency*, "American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy" 2013, issue 35, no. 1.
128. K. Giles, *"Information Troops" – a Russian Cyber Command?*, w: *Third International Conference on Cyber Conflict*, C. Czosseck, E. Tyugu, T. Wingfield (ed.), Tallinn 2011.
129. *Контрразведывательный словарь*, Москва 1972.
130. T.D. Schuman (J. Bezmienov), *Love Letter to America*, Los Angeles 1984, pp. 17–46. Compare: idem, *No "Novosti" is Good News*, Los Angeles 1985;
131. *World Thought Police*, Los Angeles 1986.
132. T.L. Thomas, *Russian Views on Information – Based Warfare*, "Air and Space Power Journal" 1996, issue 115.
133. *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*, "Journal of Slavic Military Studies" 1998, issue 11.
134. *Nation-state Cyber Strategies: Examples from China and Russia*, in: *Cyberpower and National Security*, F.D. Kramer, S.H. Starr, L.K. Wentz (ed.), Washington 2009.
135. T.L. Thomas, *Russia's Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI, the State Technical Commission and the Military*, "European Security" 1998, issue 7.

136. T.L. Thomas, *Russian Information Warfare Theory: The Consequences of August 2008*, in: *The Russian Military Today and Tomorrow. Essays in Memory of Marry Fitzgerald*, S.J. Blank, R. Weitz (ed.) Carlisle 2010.
137. P.A. Goble, *Defining Victory and Defeat: The Information War Between Russia and Georgia*, in: *The Guns of August 2008: Russia' War in Georgia*, S.E. Cornell, S. Frederick Starr (ed.), New York–London 2009, M.E. Sharpe.
138. S.J. Main, *The 'Brain' of the Russian Army: The Centre for Military-Strategic Research, General Staff (TsVSI GSh), 1985–2000*, "Journal of Slavic Military Studies" 2000, issue 13.
139. С.Г. Чекинов, *Центр военно-стратегических исследований Генерального штаба Вооруженных Сил Российской Федерации. История и современность*, "Военная мысль" 2010, issue 1, pp. 3–5; K. Giles, A. Monaghan, *Russian Military Transformation. Goal in Sight?*, Carlisle 2014.
140. С.Г. Чекинов, С.А. Богданов, *Асимметричные действия по обеспечению военной безопасности России*, "Военная мысль" 2010, issue 3.
141. T.L. Thomas, *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?*,„Journal of Slavic Military Studies" 2014, issue 27.
142. Я.Д. Короход, *Информационно-психологические войны – оружие XXI века*, "Актуальні проблеми політики" 2013, issue 50.
143. С.Н. Бухарин, В.В. Цыганов, Ю.Г. Бочкарева*, Провокации в информационном противоборстве*, "Информационные войны" 2013, issue 1.
144. В.В. Цыганов, В.В. Васин, С.Н. Бухарин, *Интеллектуальные механизмы информационных войн*, "Проблемы управления" 2007, issue 1.
145. С.Н. Бухарин, Ю.А. Матвиенко, *Информационно-психологическая война как одна из форм разрешения социально-политических противоречий в современном обществе*, "Информационные войны" 2008, issue 4.
146. H.S. Rothstein, *Strategy and Psychological Operations*, w: *Information Strategy and Warfare. A Guide to Theory and Practices*, J. Arquilla, D.A. Borer (ed.), New York 2007.
147. П. Лайнбарджер, *Психологическая война. Теория и практика обработки массового сознания*, Москва 2013.
148. A. Wilk, *Rosyjska interwencja wojskowa na Krymie* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [availability: 16 VIII 2014].
149. T. Iwański, W. Rodkiewicz, A. Wierzbowska-Miazga, A. Wilk, *Rosja wobec Ukrainy: nie tylko Krym* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-12/rosja-wobec-ukrainy-nie-tylko-krym [availability: 16 VIII 2014].
150. В.В. Квачков, *Применение Войск Специального Назначения в современных условиях*, in: *Спецназ ГРУ. Очерки истории. Кн. V: Новейшая история 1999–2010 гг.*, С.В. Козлов и др. (ed.), Москва 2010.

151. *Некоторые положения теории специальной операции и необходимость Сил Специального назначения в составе ВДВ*, in: *Спецназ ГРУ. Очерки истории. Кн. V: Новейшая история 1999–2010 гг.*, С.В. Козлов и др. (ed.), Москва 2010, pp. 393–404. Compare: И.Н. Воробьёв, *Информационно-ударная операция*, “Военная мысль” 2007, issue 6.
152. Г. Почепцов, *Информационные операции и Крым: базовые причины для манипуляций* [online:], http://psyfactor.org/psyops/infowar_krym.htm [disponibilitate: 16 VIII 2014].
153. idem, *Информационные операции и Крым: причины и следствия. Часть 2* [online], http://psyfactor.org/psyops/infowar_krym2.htm [availability: 16 VIII 2014].
154. W. Hays Parks, *Special Forces’ Wear of Non-Standard Uniform*, w: *International Law Studies. Issues in International Law and Military Operations*, J.B. Jaques (ed.), Newport 2006.
155. P. Nord, *L’intoxication par une intoxicateur*,w: *La désinformation: Arme de guerre*, V. Volkoff (ed.), Lausanne 2004.
156. Л.В. Савин, *Украина в сетевой войне*, “Информационные войны” 2008, issue 3.
157. S.J. Cimbala, *Sun Tzu and Salami Tactics? Vladimir Putin and Military Persuasion in Ukraine, 21 February–18 March 2014*, “Journal of Slavic Military Studies” 2014, issue 27.
158. J. Berzins, *Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Riga 2014.
159. M. Vázquez Liñán, *Putin’s Propaganda Legacy*, “Post Soviet Affairs” 2009, issue 25.
160. *Молот Правды. Жителям Юго - Востока: инструкция по самоорганизации* [online], http://rossia3.ru/quotes/all/9007 [availability: 16 VIII 2014].
161. T. Iwański, M. Menkiszak, *Prorosyjski “separatyzm” narzędziem przymuszenia Ukrainy do federalizacji* [online:], http://www.osw.waw.pl/pl/publikacje/analizy/2014-04-09/prorosyjski-separatyzm-narzedziem-przymuszenia-ukrainy-do [availability: 16 VIII 2014].
162. Р. Скоморохов, *Портреты века: Игорь Стрелков*, “Военное обозрение” dated 20 V 2014 [online], http://topwar.ru/48026-portrety-veka-igor-strelkov.html [availability: 16 VIII 2014].
163. Д. Виноградов, *Боевые заслуги: кто научил воевать Игоря Стрелкова*, “Свободная Пресса” dated 5 VII 2014 [online], http://svpressa.ru/society/article/89194/?rss=1 [availability: 16 VIII 2014].
164. А. Черкасов, *Игорь Стрелков в Чечне. 2001 год, Веденский р-н,* Радиостанция «Эхо Москвы» от 21 мая 2014 [online], http://www.echo.msk.ru/blog/shalommani/1324504-echo/ [availability: 16 VIII 2014].
165. Министерство обороны РФ, *Разведывательная Подготовка Подразделений ВДВ*, Москва 1995.

166. *Сводки от Стрелкова Игоря Ивановича. Сообщение от ополчения* [online], http://vk.com/strelkov_info?w=wall-57424472_5439 [availability: 16 VIII 2014].
167. С. В. Козлов, *Противостояние*, w: *Спецназ ГРУ. Очерки истории. Кн. IV: Безвременье. 1989–1999гг.*, С.В. Козлов и др. (ed.), Москва 2010.
168. Żochowski, P., Wilk, A., Konończuk, P. *Konflikt w Donbasie – wymuszona deeskalacja?* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-06-11/konflikt-w-donbasie-wymuszona-deeskalacja [availability: 16 VIII 2014].
169. *Noworosja: "Jowan Szewicz" rośnie w siłę* [online], http://xportal.pl/?p =15319 [availability: 16 VIII 2014].
170. Учитель, М. *Александр «Варяг» Матюшин: нам нужна республика нового типа* [online], http://rossia3.ru/politics/vatjag_matyushi [availability: 31 VII 2014].
171. Публичная интернет-библиотека Владимира Прибыловского, *Евразийский Союз Молодежи* [online], http://www.anticompromat.org/esm/esm_spr.html [availability: 31 VII 2014].
172. Евразийский Союз Молодёжи, *Помощь Донбассу, записаться добровольцем!* [online], http://rossia3.ru/news/2014/05/14/12:37:24 [availability: 31 VIII 2014].
173. Sykulski, L., (2014), *Koncepcja Radykalnego Podmiotu i "czwarta teoria polityczna" Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejskiej*, "Przegląd Geopolityczny", issue 8.
174. Dugin, A.G., (2014), *The Multipolar World and the Postmodern*, "Journal of Eurasian Affairs", issue 2.
175. Публичная интернет-библиотека Владимира Прибыловского, *Коровин Валерий Михайлович* [online], http://www.anticompromat.org/esm/korovbio.html [availability: 31 VIII 2014].
176. *Катехизис члена Евразийского Союза Молодежи* [online], http://www.rossia3.ru/katehizis.html [availability: 31 VIII 2014].
177. Arquilla, J., Ronfeldt, D., (2001), *The Adwent of Netwar (Revisited)*, in: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, J. Arquilla, D. Ronfeldt (ed.), Santa Monica.
178. *Евразийские боевики из Восточного Казахстана?* [online], http://z001.kz/news/view?id=1700 [availability: 31 VIII 2014].
179. Tomasiewicz, J. (2009), *Strategia oporu niekierowanego w wojnie asymetrycznej*, "Przegląd Geopolityczny", issue 1.

SECURITY PARADIGMS IN THE 21ST CENTURY

THE INFORMATION SECURITY ENVIRONMENT: CYBER-ATTACK AS THE MODERN 21ST CENTURY THREAT

Raisa Gabriela ZAMFIRESCU[*]

Motto

„The new century risks being overrun by both anarchy and technology.
The two great destroyers of history may reinforce each other."
(Cooper, 2007)

Abstract

The 21st century began with remarkable discoveries in countless fields, it has brought along a technological evolution unheard of but, together with the positive aspects the negative ones have appeared, the latter being defined by specialists as pervert aspects. Certainly one of the greatest challenges is the one in computing where, according to Eric Schmidt, CEO of Google, starting of 2010, in 48 hours there is produced as many information as before 2010, but it is not knowledge what it is being produced, most of the registered data being noise, reason for which, generally speaking, information services and security structures must re-evaluate the paradigm, the operating mode, the working methodologies and instruments. This evolution had and it still has a powerful contribution in transforming and modernizing the risks and threats to the security of a state, asymmetry being presently a success feature for the malware attacks of the new century; most times it is this feature that succeeds in ensuring the necessary strategic advantage.

Keywords: security, intelligence, Digital Age, hybrid warfare, cyber attack.

Introduction

One of the known theorems of sociology, when it comes about society and community, belongs to Herbert Spencer (*British Encyclopaedia*, 2014) who, in his research activity both in biology and sociology, formulated the theory according to which society is like a biologic organism, that appears/takes shape, grows/ evolves, ages and then dies/disappears.

[*] "Mihai Viteazul" National Intelligence Academy.

Society is in a continuous evolution and change, a fact which we cannot stop or remove, all that remains us to do is to accept, to understand and to work in order to prevent what we can prevent and to maintain national security, but also to fulfil the role our state has in the bilateral partnerships, alliances and international structures it is a member of.

What happened before 1990 has helped us to understand conventional threats, to be able to classify and define them, to formulate a basis frame and a model of analysis which we could relate to at present, in this attempt to define and label the atypical and the unpredictable. It is not a pattern easy to achieve, but it is certain that there is an attempt to constantly update it, being periodically round up by the quotidian which we define as a state of stability and by the actions taken which don`t fall under the construct of security (with all its branches).

Ever since this constant evolution of technology appeared, society found itself confronted with new challenges, the academic environment beginning to study and develop new branches, such as netnography[1], cyber culture, digital ethnography, while the security sector comes into contact more and more often with malware attacks of a cyber-nature. A good example may be the cyber-attack against SONY Pictures Entertainment launched at the end of 2014, a case whose consequences extended beyond the entertainment industry and the impact upon the ones involved, by invading the correspondence and by publishing personal character data, getting step by step to the presidential administration of the United States of America, the signing of a trilateral agreement and last but not least, to a series of threatening declarations on behalf of North Korea.

The aim of this endeavour is to draw attention on the evolution of the security environment in the 21st century and on the new threats which we are confronting both individually and collectively, as a society, pointing also out the defining elements and the repercussions of the attack from SONY Pictures, an investigation still in progress and a moment seen as critical, a moment which changed the modern Hollywood.

[1] Netnography is the branch of ethnography which analyses the behavior of netizens in their online performance, deeming that through the high degree of anonymity and accessibility all interactions that take place on the virtual field are defined as more profound and more complex than the real ones, these aspects being due especially to the lack of consequences. The term was used first by Robert V. Kozinets and it defines a method more rapid and a more accessible to researchers, more naturalistic and more discreet than many other research methods, offering information about language, behavior, customs, symbols, senses and various cultural perspectives.

Security environment

State security is “an imprescriptibly right which derives from the full sovereignty of the people, it is founded on the constitutional order (…), it has the national values, interests and objectives as a reference field.” (Romania`s Strategy of National Security, 2007, p. 7). Briefly, it can be defined as the protection of the values, the interests and the objectives of the existence of a state but, before assigning it to the category of fundamental rights, security can be defined briefly as a situation depending upon the structure of each system, having a set of characteristics and a series of paradigms which have remained unchanged before the human evolution and the transition of the post-industrial society to the modern one, evolving subsequently to the information society, making at present the transfer to the knowledge society- with a series of paradigms which can be found at the level of the entire living material because it is not only the state that requires security, it is also the individual, at a biological level.

On its turn, the security environment may be defined as an assembly of activities, actions and concerns which point out the security stage, whose main influencing factor is the globalization, process which led and it still leads to the evolution and the innovation of the national and international threats. In the last 25 years, the threats on the contemporary security environment modified both their character (the possibility of an attack from other democratic states is reduced, for that reason we must take into account threats coming from some non-state and cross-border actors), and the way of showing , the latter being defined especially by innovation, by events like the Black Swan – unexpected and unforeseen events from the social life which must be rare, must have a special impact, through subsequent consequences, but also a low degree of predictability (Taleb, 2010, pp. 5-17). One of the more common examples of this type of events is certainly 9/11. What happened on September 11, 2001 has generated numerous scale consequences on all levels and sectors of the American society, inclusively the change of the security paradigm at a worldwide level in an interconnected modern world. At the same time, broadcasting the events live by the mass-media led to continuously exposing the terrorism phenomenon, provoking instability both internally, for the United States of America, and externally, in the diplomatic and strategic partnerships, 9/11 becoming a media event which brought the Islam in the spotlight, together with the vulnerability of the epicentre of the worldwide capitalism, the fatidic day of America being defined afterwards by some experts as the day when the Western civilization clashed with the Muslim civilization.

By excessively and aggressively exposing the events, mass-media succeeded in creating new prejudices and stereotypes at a social level, and the panic and terror spread by the Al-Qaeda terrorists through the September 11 attempts, but also through other subsequent, similar actions, led to their defining by John Graz as "a symbol of modernity and a symptom of globalization" (Barna, 2010, p. 9).

These new atypical and asymmetric threats cannot be fought or foreseen by the states only individually; if before 1990 the characteristics of a new conventional assault were known, a state can be attacked much easier at present by launching actions in order to aim at the national economic and/or information infrastructure, an action which would only require the acquisition of some performing computer systems, with much lower costs than the equipment of an army would require. This is one of the reasons why most countries adhere and aim at alliances and economic, political and/or military partnerships, forming a new worldwide order, characterized by the fluidization of state borders.

It is to be mentioned that for these new types of threats, with an asymmetric character, by fluidization of state borders, globalization has facilitated the access to technological and information progress, it has intensified the international competition economically speaking, generating vulnerabilities for the state security through economic espionage, peculation, data theft etc., and it has led to the changing of the crosshairs of information communities on an information level (helped by the technological evolution), to the removal of the culture of secrecy and to the development of a security culture at a society level because security is a common asset and intelligence is no longer just a process and a service product; this way intelligence organizations were constrained to function in parallel, according to two paradigms, a traditional and a modern one (in continuous evolution), *need to know* becoming *need to share*, in order for the information to be valuable in real time.

Security environment has evolved and asymmetry has become a success feature for the malware attacks of the new century and for the new millennium, sometimes this very feature ensuring the awaited result. Asymmetry and irregularity of an attack, no matter the field we refer to, offers a strategic advantage for the one launching it, the novelty not being framed in any of the patterns already monitored, which is why it might be too late until certain authorized organs are taken notice to.

The 21st century began with remarkable discoveries in countless fields, it has brought along a technological evolution unheard of but together with the positive things the negative ones appeared, or, as defined by specialists, the pervert aspects. Certainly one of the greatest challenges is the one in computing where, according to Eric Schmidt, CEO of Google, starting of 2010, in 48 hours is produced as many information as before 2010, but this is not knowledge, most of the data being noise, reason for which, generally speaking, information services and security structures must re-evaluate the paradigm, the operating mode, the working methodologies and instruments, the four battle fields (air, water, terrestrial, space) become five at present - the cyberspace.

Another dimension of this revolution is rendered by the fact that at present, security is no longer just the military type, like in the past, when it existed a relation of equality between security and the military power, so that at present, when we bring up in discussion the protection of national objectives, values and interests, we point out a wide system of defence proceedings and measures out of which results a classification of the security at a political, military, societal, economic, alimentary, information level, even at an environmental level, the biosphere being the stage of all actions. It looks like an effective modality to evidence the security types, this way succeeding to establish the elements of such an analysis for each category, having a reference object and a series of involved and functional actors on each level, but they are inseparable elements of the national security construct, which is why the attacks are not the same either, that is they don`t respect the "recipe" of conventional attack or war, thus speaking of hybrid actions with implications on each level and on each bearing of the society.

Even if it is not a new modality, accepting the term of "hybrid" and a plurality of complex actions which bring into conflict two states or entities without necessarily existing a declaration or a military encounter on a battle field started new divergences, the taxonomy of this term being the one widely debated upon, in order to establish what this new hybrid form included precisely , so as to be able to find out which are the limits allowed and from which point on we are dealing with breaking the rules.

Up to this moment, the hybrid[2] war was defined as a type of war without limits, complex, with actions on multiple dimensions and a modern technology which tries to outperform the military training, which combines the conventional war, with its rules and limits, with the typical asymmetry of the 21st century, a modern form which includes action means allowing the aggressor to avoid attributing/claiming these actions, which can become clandestine attacks (Hunter and Pernik, 2015, p. 3).

The hybrid war is fought on all bearings of the society, through economic and financial actions and sanctions (embargo, commerce restrictions, delaying or cancelling certain contracts, bank accounts blocking), political (exclusion from certain organizations and alliances), diplomatic, military and last but not least on an information level, the cyber dimension representing one

[2] Hybrid – an entity coming out from the crossing of two individuals of different species, types, genres or races.

of the strengths of this new form of conflict. With a society more and more dependent upon the information systems, it was only natural that threats at this new life style, chosen and imposed at the same time, should appear.

The 21st century – the beginning of the digital era

The end of the Cold War, alongside with the globalization, led to an information revolution, causing the diversifying of risks and threats which any state must prevent and fight, the 21st century forcing the security environment to a change of paradigm, to a harmonious and efficient matching of the traditional with modernity – Eric Hrovat (2001, p. 2) highlighted very well that "the conventional war (tanks, planes, ground troops, submarines, rackets, defence systems) started being replaced by the *shootings* of binary digits, on a different battle field. The information war is the new art of sub mining the adversary in the new battles. You don`t have to be on the battle field". It is to be noticed that in the past, using non-conventional fight means defined you as a weak opponent which fought dirty, taking advantage of the vulnerabilities of the opponent, but it is precisely what led to one`s own denigration that is now being considered as an intelligent strategy.

This century is a digital one and information is a weapon which can kill, the power belonging to the one who owns it. We are living in an information society where everything is made online, according to the modern rite, we have Wi-Fi connexion wherever we went, tablets and/or smart phones have already become a *must have* and even if we don`t use them up to their real capacity, they still represent trustworthy instruments when it comes about social networks and the lack of self-induced privation alongside with the check-ins or the pictures posted in order for your friends (and not only them) to see how much fun you are having, how you get bored, where you are traveling, which are your hobbies or any other thing more or less insignificant that you are thinking of. Some might say that the Internet is a gift from God for psychos and bad intended persons (criminals and/or harassers), this evolution making their *work* easier for sure. Based on these facts we can state that the events on September 11, 2001 have demonstrated how the positive aspects of globalization, with everything the West is presenting as evolution and modern technology, can be used in a negative way and destructively by the terrorists for their own cause – at the same time, it is to be mentioned that one of their recruiting strategies consists of presenting the materials found online, where one can find elements of violence, corruption, abuse, citizens` deprivation of liberty in the name of the national security, destroying, poor people lacking any help or material support, briefly, "images of despair"(Barna, 2010, pp. 7-20).

The Pirates of the Internet: #GOP and the SONY Pictures attack

The last quarter of the century has led to a technological development unheard of, which contributed to the formation of a cyber-community which activates in a space without geographic/physical borders, the cyberspace, whose battle field is the Internet and the frequently updated arsenal is rendered by the New Media (The OSINT Guide, 2012). If after the attacks on September 11, 2001, the press was invaded by articles having the air pirates at the centre, in the last years and as a consequence of the global war fought against terrorism, their notoriety decreased and the pirates of the Internet stepped in the spotlight, cyber-attacks growing in number considerably.

A new taxonomy of the cyber terms rapidly structured in order to frame the actions of the soldiers on the new battlefield, so that the majority of conventional techniques get the prefix of "cyber", being created terms such as cyberintelligence, cyberwarfare, cyber manipulation, cyber infiltration, cyber assault, cyber-crime, cyber raid, cyber-attack (Alford, 2000, p. 105).

There is still confusion in defining and categorizing information attacks and cyber-attacks of a terrorist type, thus, even if both types of attacks develop on the same battle field, there is a series of considerable differences between them, the most important being rendered by the main characteristic of a terrorist attack that is causing victims. A complete definition for cyber terrorism which can be considered as the main distinction between this modern form of terrorism and the cyber-attacks is delivered precisely by the Federal Bureau of Investigations (FBI), which describes the cyber terrorism as "the deliberate attack against information, information systems, information programs and data, motivated politically, resulting in violence against non-combat targets, by sub national groups or clandestine agents."(Alford, 2000, p. 105)

Cyber-attack is one of the most serious information threats which aim at the virtual reality of this on/offline universe of the 21st century, attack which can be launched with software means, with password attack specific products, with identification codes, with electronic mail-actions without present rules which aim at modifying and/or destroying data bases or different products by tracking system vulnerabilities, security breaches and data theft. Such cyber-attacks can aim at the presidential sites (Ukraine, 10.2007)[3], stock sites, bank sites, embassy sites (August 1997)[4] or official

[3]Ukraine, 10.2007: the cyber-attack on president Viktor Iuşcenko's website launched by the young wing of the Movement for Eurasia that blocked the website for 3 days;

[4]August 1997: the block of several embassies from Sri Lanka sites for two weeksby the Black Tigers Group, a group related to the Liberation Tigers from Tamil Eelam, by overloading the electronic mail with more than 800 emails.

pages of the public institutions and not only, and can easily escalate from activism and hacktivism to cyber terrorism if they attacked the critical infrastructures and then blocked the emergency services, if they sabotaged the information, financial, electrical, transportation networks etc. Terrorists could use the cyberspace at the same time, in order to amplify the effects of conventional attacks. The advantages of the cyber-attacks could be found in the anonymity of the attacker, in the lack of geographical borders, in the accessibility and in the low costs of the equipment and last but not least, in the popularity which can be acquired easily by ensuring a witnessing public, an audience which can rapidly be transformed in a target.

The soldiers of the new *battle field* are divided in different categories of the black hat/white hat hacker[5] type, crackers[6], they have their own language (*leet*)[7], fighting techniques personalized according to the filed they activate in – phishing[8], spoofing[9], juice hacking[10] etc., and last but not least, the instruments/the weapons necessary for the malware attack-botnets, virus or informational worms which take advantage by those zero-day[11] of the equipment used worldwide. Deep Web or Dark Web have become terms known by most people, even if getting into these zones of the internet requires extensive knowledge in the field.

The most recent cyber-attack which was on the headlines in the United States of America is the one against SONY Pictures Entertainment at the end of 2014, not even three years after the attack of Sony PlayStation which caused serious financial and image damages. We mentioned previously that such attacks have grown in numbers, reason for which it must be reminded that in September 2014 Apple was hacked, more pictures (mostly nude) of famous stars from Hollywood being stolen from the iCloud system and made public. Threats continued and after the SONY Pictures information system from

[5] Black hat hacker: a person who illegally accesses the software of some devices with malicious intent. White hat hacker: a person who legally accesses the software of some devices, being an expert in information security.

[6] Cracker: a person who practices exclusively password cracking and/or their subsequent change;

[7] The new *leet* alphabet used in a closed gamers and hackers community in the cyberspace in order to make their activity more difficult to detect;

[8] Phishing: the act of sending fraudulent emails in order to infect devices they are accessed from with the purpose of stealing stored information

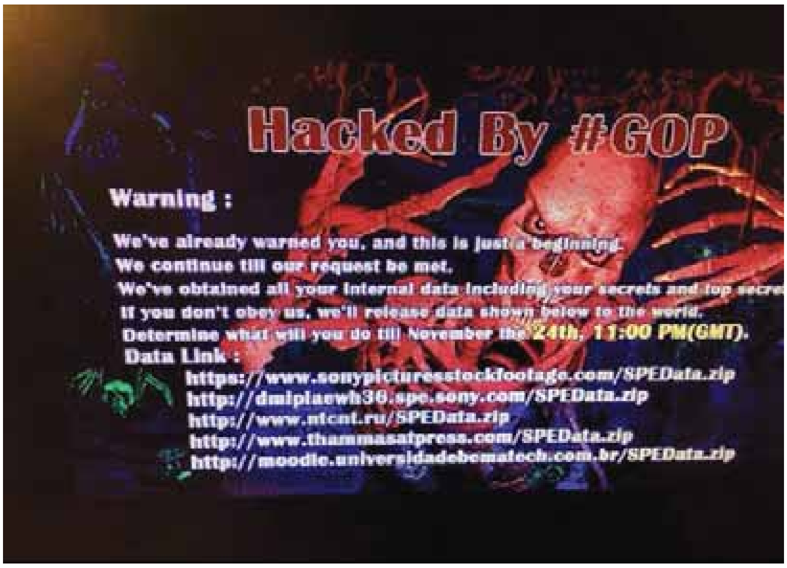
[9] Spoofing: the action a program or a device is being manipulated by, in order to look and act like another, with a fraudulent purpose;

[10] Juice hacking: a fraudulent intrusion by using an USB power cable, an action a malware can be installed and/or accessed by or information can be copied by. The vulnerable devices are the smart type (phone, tablet);

[11] Zero-Day: a vulnerability in the software of the devices unknown to the manufacturers which can be exploited by hackers;

Cluver City was blocked and subsequently closed for safety reasons and for investigations and the employees had to return to working with pencil and paper, on November 2014, another entity attacked the Playstation service but the Xbox consoles from Microsoft also. After it was settled that the two attacks had different authors, what happened in November was claimed by the group called #GoP aka Guardians of Peace and in December by the Lizard Squad, a virtual entity whom we don`t know at present if it is a group or a single individual, but we can say that it is "of honour", because it announced even from the beginning of the month that a Christmas present would be next.

Briefly, what is being considered as the biggest information attack began on November 2014, when the employees of Sony Pictures from Culver City received a message which blocked the information system (phones, e-mail, PCs), on the desktop appeared a picture with a skeleton, the title "Hacked by #Gop"(see figure 1). For the moment they did not specify the reason of the attack, but the estimated damage was the theft of approximately 10 TB (terabytes) of confidential and strictly confidential data from the Sony Pictures servers.



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

Figure nr. 1 – The message received by Sony Pictures' employees on 24.11.2014
Source: https://pmcdeadline2.files.wordpress.com/2014/11/hacked-by-gop-sony-pictures-under-attack.png?w=970

After a three day of silence, a new action from the hackers followed, the GoPloading on the online hubs aka Torrente five new movies of the studio-these have been extracted on the attack on 24th, being promotional type DVD versions. Out of the five Sony productions, only one had been released up to then, that is the movie “Fury”, featuring Brad Pitt, this production becoming rapidly the second most pirated movie, with over 1 million downloads with unique IP addresses. Together with this movie there have been posted also complete versions of four movies about to be released: “Annie”, “Mr. Turner”, “Still Alice” and “To Write Love on Her Arms”.

On November 28th there appeared the first speculations that it was exactly North Korea who was behind the cyber-attack launched by the group called Guardians of Peace, a connexion with the premiere of the comedy “The Interview” being made and on December 1st the Internet was once again bombarded with confidential information stolen from the servers of the Sony Pictures company-production budgets, passwords, security protocols, information about stars, their nicknames used for reservations, birth dates, addresses, employees` social insurance numbers and not only, the salaries of the 17 best paid officials of the company, but also of another 47.000 employees and collaborators and last but not least, a series of e-mails within offensive conversations about some famous names from Hollywood, but also about president Barack Obama (Mediafax.ro).

After this action, the Sony Pictures managers, Michael Lynton and Amy Pascal, made the first official declarations, defining the attack as a malware attack and the FBI was also involved. Things have escalated little by little and investigations are in progress, but even if North Korea continued to deny vehemently its involvement in the cyber-attack launched by the GoP, the investigators succeeded to track a series of virtual residues, identifying them as belonging strictly to the systems and servers accessible in North Korea only – information delivered at the end of December in a declaration of the FBI director, James Comey (Agerpres.ro, 07.01.2015).

The central piece of the entire cyber-attack is the Sony Pictures production “The Interview”, a comedy with a 44 milion $ budget, which represents a fictional assassination attempt on the North Korean leader Kim Jong-un. The movie was controversial from the very beginning, even from June 2014 Phenian requesting to be blocked. Not accepting the censorship imposed, Sony postponed though the premiere from October, making a series of changes of the end of the movie, regarding the death of the dictator. After four modified versions and even after the SONY Japanese president Kazuo Hirai consented, producer and actor Seth Rogen considered that “this is now the story of the Americans who change the movie in order to make North Koreans happy. It is a disgraceful story.” The actor wrote in an e-mail to the Sony co-president, Amy Pascal, a conversation made public by the GoP (Mediafax.ro).

The decision of the studio not to postpone the premiere led to a new series of threats from the hackers, after which the FBI warned the theatres regarding possible attacks; the official release of the movie was cancelled, this action causing a wave of discontent at Hollywood, but also among the presidential administration and it was seen as an act of surrender: *"Soon, the world will see the bad movie that Sony Pictures Entertainment has made. The world will be full of fears. (…) Remember September 11, 2001. We recommend you to keep away from those places (where the movie is projected). And if your place is in the nearby, you should leave home. All that will happen in the next days will be SPE`s fault. The entire world will denounce Sony* "(Mediafax.ro).

Conclusions

Even if they thought everything was lost, the entire publicity and controversy started a real war for freedom of expression in a democratic state and the movie got to be projected in over 500 independent cinemas from the United States of America, on January 8th, 2015, with a box office of approximately 5 million $ and it was made available to the public online, on the most famous platforms, for renting or buying. The sites that streamed the movie were GooglePlay, YouTube Movies, Xbox Video Microsoft and the official page www.seetheinterview.com, and Apple joined them on December 28thwith the service iTunes. On January 8th, the comedy got to earned 31 million $, with a final box office of 38 million $ from the online broadcasting with prices of 5.99 $ and 14.99 $ and "The Interview" became the no.1 online movie of Sony Pictures.

The consequences were immediate and a series of coincidences simply strengthen some people`s suspicions that they had been planned. Even if there are still conspirationists who place the attack as a marketing strategy of Sony in order to promote a second hand movie (which succeeded to divide the world of critics in two camps), escalating tensions between the United States and North Korea and the involvement of the FBI also seem to contradict this hypothesis. A series of demission took place at Sony Pictures Entertainment and more employees filed a common complaint because their personal and confidential information was not protected – a message posted on the official site by Sony (www.sonypictures.com). A series of declarations began at an official and diplomatic level, president Barak Obama defining the cyber-attack as an act of vandalism which will bring about retribution for the culprits (even re-inclusion on the list of states which support terrorism being taken into account; North Korea had been removed from that list in 2008, after George W. Bush had nominated the state on the axis of evil, together with Iran and Iraq, while leader Kim Jong–un and his administration launched a series of threats and offenses, which is the reason why some specialists consider that this is the beginning of a cyber-war between the two nations.

> *"Our most hard counter attack will aim the White House, the Pentagon and the American continent, the septic tank of terrorism and will be much more than the " symmetric counter attack" announced by Obama* "- the National North Korean Defence Commission (NDC)(Agerpres, 21.1.2.2014).

A first reaction from the USA was a massive interruption of the internet and 3G connexion between North Korea and the other states, these retributions not being admitted officially, but accepted in the very declaration of the spokesman Maria Harf: "(...) among our responses, some will be visible, other will not". They continued with the signing of a trilateral agreement between the United States of America, Japan and South Korea, this agreement regarding the exchange of confidential data on the nuclear project of Phenian, which foresees that any confidential information be transmitted to the two Assian countries through Washington (Agerpres.ro, 26.12.2014). Another decision made by president Barack Obama – this time applicable internally- is the revision and consolidation of the cyber strategy of the United States.

Investigations are in progress, Sony Pictures is trying to fix what can be fixed, the fight being now at the level of the presidential administration. It is certain that cyber-attacks have become a major problem for the current society and these attacks can escalate in real global problems, especially since the means which can be used as main weapons by the internet pirates are indispensable devices in the everyday life of the 21st century, the digital era.

References:

1. *Agerpres – Actualizează lumea. Sony Pictures*. http://www.agerpres.ro/views/site/pages/content/searchResults.html?q=sony+pictures [Online] (accesed 6-8.04.2015).
2. Agerpres.ro: http://www.agerpres.ro/externe/2014/12/21/phenianul-ameninta-washingtonul-cu-represalii-daca-sua-vor-sanctiona-rpdc-in-scandalul-sony-18-47-42 .
3. Agerpres.ro: http://www.agerpres.ro/externe/2014/12/26/acord-sua-japonia-coreea-de-sud-pentru-schimb-de-date-confidentiale-vizand-programul-nuclear-nord-coreean-14-27-50.
4. Agerpres.ro: http://www.agerpres.ro/externe/2015/01/07/directorul-fbi-hackerii-au-fost-neglijenti-in-atacul-informatic-asupra-sony-si-au-folosit-servere-nord-coreene-20-39-27.

5. Alford JR., Lionel D., (2000), *Cyber Warfare: Protecting Military Systems.* [Online] http://www.dau.mil/pubscats/pubscats/AR%20Journal/arq2000/alford.pdf (accessed at 7.04.2015).
6. Antipa, Maricel, (2010), *Triumviratul dezastrului global*, Bucureşti: Editura Monitorul Oficial.
7. *Analiza de intelligence,* (2013), Curs nepublicat, susţinut în cadrul prelegerilor de Analiza Informaţiilor: OSINT în cadrul Facultăţii de Sociologie şi Asistenţă Socială, Universitatea din Bucureşti.
8. Barna, Cristian, (2010), *Terorismul, ultima soluţie? Mărirea şi decăderea Al-Qaīda*, Bucureşti: Editura Top Form.
9. Cooper, Robert, (2007), *Destrămarea naţiunilor. Ordine şi haos în secolul XXI*, Bucureşti: Editura Univers Enciclopedic.
10. Deadline.com, (22 december 2014), *Sony Hack: A Timeline.* [Online] http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ (accessed at 6.04.2015).
11. *Encyclopaedia Britannica*, (2014), *Herbert Spencer*. [Online] http://www.britannica.com/EBchecked/topic/559249/Herbert-Spencer (accessed at 10.04.2015, 10:17).
12. *Ghid OSINT*, (2012), [Online] http://www.sri.ro/upload/Ghid_OSINT.pdf (accessed at 4.04.2015).
13. Hrovat, Eric, (2001), *Information Warfare: The Unconventional Art in a Digital World*. [Online] http://www.sans.org/reading_room/whitepapers/warfare/information-warfare-unconventional-art-digital-world_787 (accessed at 6.04.2015).
14. Hunter, Eva şi Pernik, Piret, (2015), *The Challenges of Hybrid Warfare.* [Online] http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf (accessed at 7.05.2015).
15. Kozinets, Robert V., (2010), *Netnography: Doing Ethnographic Research Online*, London: SAGE.
16. Mediafax.ro. *Sony*, http://www.mediafax.ro/tags/sony [Online], (accessed at 6-8.04.2015).
17. Mediafax.ro: http://www.mediafax.ro/cultura-media/sony-pictures-incearca-sa-diminueze-unda-de-soc-dupa-atacul-informatic-asupra-serverelor-sale-13718290.
18. Mediafax.ro: http://www.mediafax.ro/life-inedit/filmul-despre-kim-jong-un-scena-mortii-liderului-nord-coreean-considerata-inacceptabila-si-modificata-de-mai-multe-ori-video-13723225.
19. Mediafax.ro: http://www.mediafax.ro/externe/piratii-cibernetici-au-amenintat-studiourile-sony-evocand-atentatele-din-11-septembrie-2001-13725818.
20. Petrescu, Stan, coord. (2007). *Asimetriile prezentului – Contraterorism vs. Terorism. Terorismul cibernetic*, Bucureşti: Editura Academiei Naţionale de Informaţii.
21. http://www.sonypictures.com/corp/notification/SPE_Cyber_Notification.pdf?#zoom=100.

22. *The 2014 Counterterrorism Calendar. Modus Operandi – cyber-attack*, (2014), Bucureşti: Serviciul Român de Informaţii, 2014.
23. Taleb, Nassim Nicholas, [2007] (2010), *Lebăda Neagră. Impactul foarte puţin probabilului*, Bucureşti: Editura Curtea Veche.

THE WORLD AS SEEN BY VLADIMIR PUTIN

Teodora DOBRE[*]
Virginia ANDREI[*]

Motto
"Gentleman, the vote is 11 to 1, and the 1 has it!"
(Abraham Lincoln)

Abstract

At a strategic level, the psychological assessment of the political leader becomes primordial for a successful intelligence service, mostly because we often view a nation's foreign policy in terms of its leader's personality and we know that their decisions are influenced by their belief system (or operational code) and motivations. This paper is focused on shaping a connection between the operational code of Vladimir Putin and his actions, taken in the name of Russia, managing global crises like the American invasion in Iraq, the Iranian file, the missile defence problem, and the crisis in Syria and Ukraine. This paper seeks to discover a pattern of action within the political behaviour of the most controversial leader of the moment, as well as to develop predictions, concerning his future approaches on global issues.

Keywords: Vladimir Putin, political behaviour, political leader, international crises, cognitive system

Introduction

Understanding the phenomena of foreign policy requires a profound knowledge of the intentions and capabilities of one state and the relations it establishes in the international arena is given not only by analysis (Tetlock & McGuire, 1986, p. 152). For instance, the Soviet invasion in Afghanistan acquires various meanings depending on the assumptions regarding the Russian intentions (was this military act a defensive one, in the attempt to prevent an Islamic diffusion in Central Asia, or an offensive one, in which the

[*] "Mihai Viteazul" National Intelligence Academy.
[*] Romanian Intelligence Service.

deployment of forces in the Persian Gulf had a single goal – to obtain supremacy in the region?). The American perspective offers various answers, related and sustained by subjective arguments, like Russia's motivation and capabilities and the reasoning of the American political leaders about which are their vital interests are and what policies can be implemented in order to protect them.

These cognitive patterns are used by political figures in understanding and coding new information in scenarios, operational codes, cognitive schemes, and prototypes. They can offer inside explanations regarding the purpose and the cause of a political event and the true intention that lies behind a state's foreign policy, because they emphasize the centre of each national actor – the man that rules the country and shapes the architecture of the state.

This paper addresses, in a complex approach, the cognitive patterns of the political leader – the operational code, integrating the data as it is perceived by him under the shape of cognitive images that function in a simple process of input-output. Pursuant to interpretation, an answer is offered on how to manage properly the political status quo.

The study commences with a detailed disquisition on the concept of operational code, and outlines, from a "cognitive" perspective, the international crises managed by Vladimir Putin (from the Iraqi war in 2003, the dispute over the Iranian nuclear file, the dilemma of the NATO ballistic missile shield, to the Ukrainian crisis). It attempts to identify the behavioural pattern, the motivation and the cognitive style of the political leader that was behind every important decision in the Russian foreign policy in the last decade – Vladimir Putin.

Operational code – evolution, definition, utility

Nathan Leites (1951) coined the concept of *operational code* in political psychology, describing it as being a set of rules considered necessary for an efficient governance and followed closely by the members of the politburo. His study focuses on the writings of Lenin and Stalin and presents the way relationships are established between members of the Communist Party and individuals outside it. The purpose of his study was to identify a pattern of creating and implementing these rules, in order to be able to predict the Bolshevik decisions (Leites, 1951, p. 11). According to the Bolsheviks, all significant political events can be explained by the Marxist-Leninist law, and no event is random. The person considers that an event is the result of other forces than the political transition forces from capitalism to communism are considered to be a political Philistine (Leites, 1951, pp. 11-19). Leites identified a pattern of the Bolshevik view on power. The lack of power generates a real danger for the future and continuity of communism. This idea explains the aggressive attitude of the Bolsheviks towards the great powers in the international system, which continued even after the 1917 – revolution, when they had taken over control internally. Also, from the Bolshevik perspective, one's feelings and beliefs must be controlled completely, taking into account that they can become dominant factors in one's attitude, which may produce a catastrophe: "the political activity is a war that must be approached cold-bloodedly" (Leites, 1951, p. 20). Moreover, the members of the party must maintain a clear political direction, respect their principles in any circumstances, but simultaneously, prove they are flexible and capable to adapt to the actions of the enemy and to the changes of the external political environment, so to assure a clear victory and select the best strategy for action. These defining traits of the political organism confer both resilience and ruggedness in the race for power and supremacy (Leites, 1951, pp. 32-35).

The Bolshevik cognitive pattern supports the use of violent means for developing communism, Leites' conclusions suggesting that when the Party chooses not to use violence against its enemies, it exposes itself. From this point of view, not using violence as a form of management is a greater mistake than adopting violent measures in solving a crisis (Leites, 1951, p. 51). In a general sense, the Soviets believed that the superpowers were targeting the Russian state and that their main goal was annihilating the party, by all means. Having that in mind, every group that was not controlled by the party was perceived as an enemy and the best ally was the one supervised the most (Leites, 1951, p. 57).

Alexander George took over the concept of operational code and in his paper *The Operational Code: a Neglected Approach to the Study of Political Leaders and Decision-Making* (1969) transformed the standard norms (that can be mechanically applied in decision-making) in a series of premises and conceptions regarding the political universe. The central purpose of Alexander George's paper is to examine the conceptual system developed by leaders from various cultural and institutional environments in approaching the uncertainness and risk inherent in the decision-making process (choosing objectives, strategies). This conceptual system, known as operational code, is synthetized by Alexander George in a series of answers given by political leaders that focus on illustrating their instrumental beliefs and philosophical beliefs (Alexander, 1969, p. 199).

Regarding the structure of the operational code, Alexander George designed a set of questions about the purpose of politics that covers the basic problems of knowing and acting, faced by a leader on a daily basis. The answers help define his fundamental orientation within the political universe. Concerning the philosophical content of the operational code (external references enunciated by the leader), the following questions were drafted:

1. What is the fundamental nature of politics? The political universe and the style of political opponents are conflictual or cooperative?
2. What are the leader's perspectives in accomplishing his political ambitions? Is the approach rather optimistic or pessimistic?
3. Is the political universe predictable or not? In what way and how predictable is it?
4. How much control can a leader hold on making history? What is the role of the leader in transforming and reshaping history in the desired direction?
5. What is the role of hazard in one's life and in history?

Instrumental conceptions (internal references upon the best approaches of the leader regarding political action), subsumed to the operational code, emerge to the answers from the following questions:

1. What is the best manner to select goals or objectives when talking about political action?
2. What is the most efficient way to attain a political goal (conflict/ cooperation)?
3. How are risks calculated, controlled and accepted?
4. What is the proper moment of action to promote one's self-interests?
5. What is the utility and the role of various means for promoting one self's interests?

In the attempt to develop a more refined shape of the operational code-related conceptions, Ole R. Hosti elaborated six cognitive systems, based on the philosophical and instrumental questions of Alexander George. The basic entity in Holsti's analysis is individual behaviour, as restricted by the cognitive system of the decisional maker (Walker, 1990). The model, that take over his successors, is based on the principle of cognitive consistency, from which two general statements derive:

- Beliefs present themselves in a relationship of strict interdependence, they tend to form a coherent cognitive system and
- Under the impact of specific conditions, the beliefs restrain the alternatives of the decisional power, thus influencing the final decision. Therefore, the main idea of Holsti's study is that one leader's decisions are consistent with his restrained beliefs within his operational code (Walker, 1990, p. 409).

Walter and Falkowski applied Hosti's version and studied the relationship between the operational code of American leaders and how they reacted and managed a crisis. Analysing the conceptual systems of political figures like Truman, Marshall, Eisenhower, Dulles, Kennedy, Rusk and Johnson and trying to connect the results obtained to the means used by their administration, the authors were unable to situate the leaders in one of the four categories of the operational code. In exchange, they identified various sets of combinations between philosophical and instrumental conceptions on each of the analysed subject and a pattern in the cognitive schemes – an imbrication of conception and motivation (Walker, 1990, p. 412).

These conclusions lead to creating new priorities in the study of the operational code – establishing a connection between analysing the operational code and motivational psychology, which consists in identifying the needs of affiliation and power of the leader. The analyses on the foreign policy led by the American president Woodrow Wilson in the context of the ratification of the Versailles Treaty (Walker S.) and by the secretary of state Henry Kissinger (Starr H.) remain as proof of both the cognitive and the motivational dimension of the operational code analysis.

In conclusion, both the cognitive and the motivational elements determine a coherent and complex personality of the leader, as he can express various states of mind, depending on the problem approached. This perspective suggests that mapping the operational code of the political leader should start from bottom to top, by aligning mentalities, mind sets and concepts on a specific problem rather than from top to bottom, as a series of deductions, starting from a general cognitive system. A strategy from bottom to top is the VICS method (Verbs in Context System), which helps identify strategies and tactics most likely to be adopted and implemented by world leaders in managing future foreign policy crises (Schafer & Walker, 2006, p. 27).

VICS – the analysis of the operational code at a distance

According to Snyder, Bruck and Burton (2008), those who wish to understand foreign policy decisions must have access to the *black box* of the decision-making process, which is the agents involved in the process. The most efficient method to study the decision mechanism is the analysis at a distance, based on selecting and interpreting the psychological characteristics of the leader by studying his verbal demeanour (Snyder, Bruck, & Burton, 2008).

The premise from which VICS method starts addresses the way leaders communicate. The way they relate to power and the relations of power existent in the political universe reveals their conceptions about exerting power. The method focuses on the verbs used by leaders in televised interviews or printed declarations. Depending on how the international system is perceived to function efficiently (through conflict or cooperation), political leaders use specific verbs, that are oriented to one of these two directions (Schafer & Walker, 2006, pp. 3-23).

The message conveyed by the leader is analysed and divided into the following recording units: verb, subject and object or subject, predicative and adjective. The VICS method abstracts values for 6 attributes of each recorded sentence: subject (himself or others), verb (positive meaning or negative/cooperation or conflict), tense, target and context. The indicators taken into consideration by VICS are organized by the 10 questions elaborated by George, and pursuant to interpretation and analysis, to each answer a numeric value is assigned (Schafer & Walker, 2006, pp. 33-38). For instance, for the first philosophical indicator P1 – *The nature of the political universe,* and for the first instrumental indicator I1 – *The direction of the strategy* the values scale ranges from -1 (extremely hostile) to +1 (extremely friendly), with a gradual increase in intensity (very hostile (-0,75), definitely hostile (-0,5), sort of hostile (-0,25), mixt (0), sort of friendly (0,25), definitely friendly (0,5), very friendly (0,75)). For a leader that obtains a score of - 0,21, respectively 0,41 the results are interpreted in the following manner: the individual considers the political universe as being a hostile environment and believes that a line of action based on cooperation is the best strategy in the perceived context. The interpretation of the others 8 indices of the operational code follows the exact same pattern, although, in some cases, the values scale ranges differently.

Coding the leader's public speeches can be made manually or with the support of the software *Profiler Plus*[1], designed for psychological analysis at a distance Evaluating and predicating certain beliefs, both for his image upon others (philosophical beliefs) and his own cognitive system upon different approaches of foreign policy (instrumental beliefs), we can express predictions regarding how the subject (political leader) expects others to act and how the subject is expected to act (Lo, 2003).

The operational code of Vladimir Putin

Vladimir Putin is an iconic figure of the Russian state, who promoted a controversial foreign policy through economic, social and political reforms, besides policies for internal development. Each time, he adopted a position consistent with Russia's national interests, regardless of the risks induced by promoting opposing visions. What truly lies behind his actions and his official public arguments?

The answer can be revealed by closely studying the cognitive system of the president, identifying his vision, his cognitive pattern, motivation and perception, all these being elements with a great deal of importance in the decision-making process in a time of crisis.

The fact of the matter is that Vladimir Putin IS the Russian foreign policy, planning and accomplishing the assumed objectives and deterring the development of courses of action with negative impact. He dominates completely the Russian decisional process. The interest shown by Putin in matters of foreign policy determines a personalization of foreign relations, a strict control of the events in the international arena, and a strategic direction dictated by one voice. Those who threaten or provoke his authority are eliminated. During debates and negotiations, Putin's attitude is defined best by the expression "le consensus, c'ést moi!". Furthermore, understanding the Russian foreign policy means understanding Putin's individual traits (Lo, 2003).

The president of the Russian Federation is not an isolated case, but rather, he is a product of the Russian environment, with instincts and beliefs shaped by personal experience, the massive transformation of the Russian society, the status of the Russian power within the international system, the failures and successes obtained by his predecessors and cognitive biases that

[1] Developed by Social Science Automation, Profiler Plus is a software used nowadays in media analyses, profiling and electoral campaigns. Available at: http://socialscience.net/partners/academicusers.aspx.

encumber him to perceive the world as it is, from an objective perspective (Lo, 2003).

The international crises put the leader under pressure, forcing him to make a decision and to act within temporal, contextual and informational boundaries. Having this in mind, we can state that international crises best reveal and reflect the cognitive elements of a leader. As a consequence, this chapter identifies the operational code of Vladimir Putin and validates it, having as indicators the decisions Putin made in international crisis, such as the American invasion in Iraq, managing the international reactions regarding the Iranian nuclear programme, the problems imposed by NATO's missile shield, the Syrian civil war and the Ukrainian crisis.

Crimea entrance in the Russian dominated sphere and the presence of Russian military there generated negative reactions from the United States and other western democracies. The conclusions drawn by Angela Merkel was that Putin lives in a different reality, losing contact with what is truly happening. This observation made by the German chancellor only confirms the differences in perception that exist between West and East. Reality is perceived differently, being filtered individually and shaping different visions, attitudes, and conceptions: *We have always been proud of our nation. But we do not claim to be any sort of superpower with a claim to global or regional hegemony; we do not encroach on anyone's interests, impose our patronage onto anyone, or try to teach others how to live their lives. But we still strive to be leaders, defending international law, striving for respect and national sovereignty and peoples 'independence and identity.* (Vladimir Putin's declaration, UN's General Assembly, 12th December 2013).

The above mentioned statement illustrates the key-elements in what regards Putin's vision upon the international system, applicable in the case of international conflicts that have the potential to affect Russian interests. Thus, the unilateral intervention of the United States in the Iraqi war is constantly criticised by Putin, the dispute regarding the nuclear file was solved due to the mediator role Russia played, the missile shield developed by USA in Europe was perceived as a threat to the integrity of the Russian state and as a destabilizer of the strategic balance of power, the transformation of the Syrian conflict in an instability exporter was avoided, thanks to the diplomatic measures implemented by the Kremlin and to the solution proposed by Putin to destroy all chemical weapons, and the Ukrainian crisis, currently developing, can be managed, from the Russian perspective, only through dialogue and cooperation and by granting Kiev the opportunity to manage its own internal instability. The behavioural pattern of the Moscow leader derives from the cognitive system he has developed during the international crises and offers the possibility to identify elements with a pre-emptive character regarding the future strategies in the international arena.

In approaching the Iraqi crisis, Putin was the heir of his predecessor, Gorbaciov. He counterbalanced the consensus reached globally concerning condemning Bagdad. His vote in the United Nations' Security Council against military intervention in Iraq hides motivations like stopping the American unilateralism, preserving economic interests in Iraq and a distinct perception of crisis management towards the one of the international community. While the majority of the states consider appealing to military means in order to solve a WMD-related problem, the Kremlin only had one viable option: maintaining the presence of UN's inspectors on Iraqi soil and constant evaluations of the potential nuclear sites.

Putin balanced between avoiding a military attack in Iraq and maintaining the economic ties with Tehran. Supporting Iran in the international arena could attract Moscow in the conflict with US and EU. Negotiations were perceived as an ideal approaching method, Russian motivations revolving around the necessity of preserving the economic relationship with Tehran. However, the support given to Iran was not constant, and conforming to international norms was considered a priority. From this perspective, Putin requested Iran publicly to align to the legal framework imposed by AIEA.

Putin perceives the ballistic missile defence system that the United States is building in Europe as a threat to Russian security. Initially, the Kremlin approached this aspect from a cooperative perspective, but taking into account the refusal of the Washington administration to create a joint defence program, Putin changed his behavioural pattern and disseminates verbal threats and accusations. The problem identified in this situation derives from the subjectivity each state handles this aspect: USA claims the ballistic missile shield has as primary goal detecting a potential ballistic missile attack from Iran, while Russia does not consider the Iranian nuclear program to be a viable threat. Hence, each side is convinced the other one does not really seek to establish a genuine relationship of cooperation in the strategic field.

In what concerns the Syrian civil war, Vladimir Putin adopted rather a neutral political position. His interests in Middle East and North Africa, and especially in Syria, are motivated by historical and geopolitical grounds. When the violence reached its peak, the UN Security Council debated the possibility of a military intervention. Russia used its veto right and proposed an alternative solution: to destroy all chemical weapons, confirming Putin's operational code, oriented to respecting international law, sovereignty and elimination of military interventions, as means to achieve peace. The similarities between the two countries regarding the sense of national identity, historical affinity, political visions and strategies support the cognitive substrate of the Russian decision-making process and confirms Putin's cognitive pattern.

The Ukrainian problem is perceived as a conflict engineered by the West and directed against the constitutional norms and the wish of the Ukrainians. Putin denies the accusations of the United States regarding the deployment of military forces on Ukrainian soil and proposes a diplomatic solution. Although his cognitive and behavioural pattern do not imply the use of force as a mean of crisis management, Putin's declaration stated that Russia will intervene, if necessary, on legitimate grounds in Ukraine.

Conclusions

Overall, the analysis of Putin's operational code reveals a cooperation-oriented leader, a man who perceives the political universe in an optimistic manner and for whom, the use of force is the last resort. He does not present himself as a leader with significant control over international events and has a medium flexibility in what concerns the transition from cooperation to conflict. The dispute revolving the ballistic missile shield reveals the most negative values of his operational code, which implies a greater risk of using force as a way of addressing the problem.

The accusations the United States made over Putin's foreign policy place Russia as being a state that uses its resources as instruments of power. From the American perspective, Putin's ambition and vision is to reconstruct the former Soviet bloc and to return to the communist ideology and principles. Also, the Americans think that Russia supports dictatorial regimes, nuclear arming and seeks to become global hegemon – statements that are gradually refuted by Putin's declaration and actions within the international arena. His decisions constantly respected until now the same principles: multi-polarity, pragmatism, democracy and legitimacy.

It remains to be seen if his foreign policy will prove to be constant and consistent with these principles in the Ukrainian conflict (maintaining the diplomatic line of action) or if Russia will stage a unilateral military intervention, which contradicts his leadership style.

The political tensions between Moscow and Washington centre on a conflict of opinions, suspicions, covert intentions and political motivations. In order to fully understand their political decisions and eliminate or reduce the degree of uncertainty, one must identify and analyse the psychological elements on which these decisions are made. As a complementary aspect, Gabrielle Rifkind underlines the importance of empathy in her book *The fog of peace,* explaining how placing ourselves in various hypostases could help us understand better how and why others act the way they do.

During a speech held on 18th March 2014, after the results of Crimea's referendum were made public, Putin used the word *ruski* (which implies ethniciy) instead of *rosiski* (which defines citizenship) on multiple occasions. This „mistake" had not been noticed before. Historian Valery Solovei interprets this detail as Putin's desire to unite all Russians into one community, implement an ideological innovation, fact that amplifies the fear of the US (Piper, 2014).

Vladimir Putin will exploit his popularity in Russia and former Soviet republics in order to protect himself and the state from the challenges and threats posed by the US. A relevant example in that sense is the case of Crimea (58, 5% of the population is Russian[2]), where the will of the population was expressed through a referendum in March 2014, the results offering legitimacy to his decision to annex Crimea. His future strategy could include a unification of all Russians, dispersed in former Soviet-republics. Soon after the annexation decision, Putin explained his foreign policy towards this region, considered vital for the Moscow administration: *„They are constantly trying to sweep us into a corner because we have an independent position. If you compress the spring all the way to its limit, it will snap back hard. You must always remember this!"*

This statement reveals, from our perspective, the main characteristic of Putin's operational code: as long as he is in charge, Russia's actions will not be defined as offensive, and violence will be the last resort, as a reaction to the international pressure coming from Western Liberal Democracies.

[2] According to 2001 statistics; available at: http://2001.ukrcensus.gov.ua/eng/results/general/nationality/Crimea/.

References:

1. Alexander, G. (1969), *The Operational Code: A Neglected Approach to the Study of Political Leaders and Decision – Making*, in *International Studies Quarterly*, no. 13.
2. Leites, N. (1951), *The operational code of politburo*, New York: Mcgraw-Hill Book Company, Inc.
3. Lo, B. (2003), *Vladimir Putin and the Evolution of the Russian Foreign Policy*, London: Blackwell Publishing.
4. Piper, E. (2014, 06. 09), *'Patriot's handbook' may give insight into Putin's thoughts*, retrieved from Reuters: http://www.reuters.com/article/2014/06/09/us-russia-putin-ideology-insight-idUSKBN0EK09Y20140609, last accessed: 06.08.2014.
5. Schafer, M., & Walker, S. G. (2006), *Beliefs and leadership in world politics*, New York: Palgrave Macmillan.
6. Snyder, R., Bruck, H., & Burton, S. (2008), *Decision-Making as an Approach to the study of International Politics* in S. Smith, A. Hadfield, & T. Dunne, *Foreign Policy, theories, actors, cases*, New York: Oxford University Press.
7. Tetlock, P. E., & McGuire, C. J. (1986), *Cognitive Perspectives on Foreign Policy*, Boulder: Westview Press.
8. Walker, S. G. (1990), *The Evolution of Operational Code Analysis*, in *Political Psychology*, vol. 11, no. 2.
9. Walker, S. G. (2007), *Coding and Scoring Operational Code Beliefs by Hand: The Verbs in Context System Manual*, New York: Arizona State University.

SECURITY STRATEGIES AND POLICIES

RISK ASSESSMENT FOR INSIDER THREAT: CRITICAL INFRASTRUCTURE, MILITARY AND INTELLIGENCE APPLICATIONS

Elaine PRESSMAN[*]

Abstract

This paper reviews background information on insider threat and provides a rationale for the development of an evidence-based analytic tool to assess the individual risk for insider threat. This tool, referred to as the RAIT is of value to security and intelligence analysts in military settings, in critical structure settings and in organizations. The tool assists analysts in resolution of doubt decisions concerning the security status of individuals whose trust status is question. It is also applicable to routine re-assessments of individuals over time. Relevant risk indicators related to insider espionage, sabotage, unauthorized disclosures of classified information and violent extremism are structured into a standardized, systematic and reliable transparent tool to permit the assessment of individual risk and the threat that individuals may represent. This paper will identify some guidelines for use and the indicators in the RAIT tool. The RAIT is consistent with best practice for risk assessment and with other internationally recognized and validated risk assessment tools. The RAIT tool supports, but does not replace the professional judgment of those mandated to provide these security decisions. This work was supported by the Canadian Department of National Defence, but the author assumes full responsibility for all content and errors.

Keywords: risk assessment of insider threat, resolution of doubt for insider threat, intelligence analysis of insiders, individual risk and threat analysis of insiders.

Introduction

Insider threats are a major counterintelligence challenge. Such threats are ubiquitous. They are especially dangerous in the Armed Services, where critical infrastructure is located, in intelligence organizations and in industrial settings where intellectual property requires safeguarding.

Insider threats include acts of espionage, sabotage, terrorism, thefts, embezzlement, unauthorized disclosure of classified information, and other

[*] Senior Fellow, Canadian Centre for Intelligence and Security Studies, NPSIA, Carleton University, Ottawa and Associate Fellow, International Centre for Counter-Terrorism-The Hague, Netherlands.

malicious and criminal acts untaken by "trusted" personnel (Bronswill and Brewster, 2013)[1]. Insider threats are of special concern because the perpetrators of these acts have been granted access to sensitive equipment, protected files, and security installations. Insiders require vetting. This scrutiny has been undertaken in most cases. Such analyses are flawed or not sufficiently sensitive, if they are not capable of identifying in advance those individuals who present a threat to the organization. Risk assessments should be regularly undertaken on employees with access to secure facilities to determine the status they pose at a given time to the agency.

Individual risk assessment for insider threat refers to the analysis and evaluation of the danger posed by "trusted employees" or "trusted contractors". The risk assessment protocol includes a set of necessary and sufficient conditions pertinent to the specific type of risk which are structured into indicators that can be measured. This provides an evaluation of each of the indicators separately, as well as an overall judgment of risk and threat based on the outcome of the individual indicator evaluation and a weighting of the information available. Information that is not available is highlighted by the presence of empty cells. This missing evidence is taken into consideration in terms of its critical importance to any risk decision and provides useful direction for follow-up information retrieval.

It is this insider risk potential that an agency seeks to mitigate or eliminate. Risk assessment has been developed to evaluate and manage "dangerousness". This danger, when applied to a person rather than a physical, biological or other hazard, is referred to as individual risk assessment. Although the methodology was originally developed in the forensic setting by psychologists interested in predicting recidivism, it has been applied to violent extremism estimations of risk and is appropriate to the individual assessment of insider threat.

Insider threats occur when access is granted to "trusted persons" who abuse the trust and betray the organization that has granted the trusted status. This "trust" has usually followed from some form of an evaluation of the individual's potential risk. The assessment was intended to ascertain the reliability, trustworthiness and loyalty of the insider. In the Military and other government installations, the expert analysis that is undertaken on individuals is often supported by information provided by intelligence agencies, as well as other relevant institutions. The level of trustworthiness, reliability and loyalty

[1] This definition is consistent with that used by the Canadian Security and Intelligence agency (CSIS). See also "The Threat Environment to 2025" – a CSIS Document obtained by the CBC.

awarded to an individual will differ based on the information provided, the positions of the individual and the final evaluation.

The methodology currently applied by analysts and the risk indicators used for individual security scrutiny may not be fully transparent, objective, rigorous and systematic. They may be based on evidence available which is insufficient and on the consideration of this information and the analyst's experience. It has been argued by threat and risk assessment experts that security assessments should employ a structured and comprehensive approach that is reliable, consistent and quantifiable rather than subjective, inconsistent and analyst dependent. Results should be reliable and generate the same outcome when different analysts perform the assessment risk assessments, when a rigorous methodology is used, will include and apply the same comprehensive set of relevant risk indicators in a systematic manner. This will correct for difference in the assessor's level of experience and any bias present. Finally, the methodology will be sufficiently rigorous so as to permit the establishment of quantifiable baselines and repeat measures of risk that can be compared (Pressman, 2009).

In cases of insiders who betray, the "risk" review was either flawed, not sufficiently time sensitive, or there was insufficient ongoing monitoring of the individuals by supervisors. Flawed assessments are often the result of superficial observation due to earlier evaluations indicating "trusted status" or due to the perceptual blindness of supervisors and colleagues. Early identification of these risk indicators can result in timely action related to the mitigation of the individual's risk (Johnston).

Background: Insider Threat in the Armed Forces, Intelligence Agencies: The Role of Law Enforcement. Insider threats are a priority of armed forces and intelligence services in any country (MOSID:00161 and MOSID:00214). Most countries have gone through restructuring of their armed forces and their security and intelligence functions in the past decades often subsequent to government established commissions who have reviewed and recommended changes to their organization and function. Despite multiple re-organizations and policy changes in the past decades, the three fundamental roles of policing, (the peace officer, the intelligence officer and the enforcement officer) remain central to the prevention, mitigation and detection of insider threats. It is the police, in the end, who enforce the law when insider incidents occur. They are users of risk assessment tools and approaches (MOSID:00161 and MOSID:00214).

In a 2013 de-classified Canadian Security and Intelligence Service (CSIS) report, insider threats were identified as a significant and current concern of their intelligence agency (Bronswill and Brewster, 2013). The espionage case of Canadian naval officer Jeffrey Delisle was identified as typifying the danger of the 'insider threat' in the armed forces. In this case of Delisle, the "insider threat" extended well beyond Canada. It involved Canada's allies, and to the intelligence information to which Delisle had access. Delisle was sentenced in 2013 to 20 year imprisonment for his acknowledged multiple acts of insider espionage that had caused damage to Canada, the United States, Australia, The United Kingdom and New Zealand. His actions were described as "severe, irreparable and exceptionally grave" (Bronswill and Brewster, 2013). What is clear is that such insider threats are both serious and credible.

Experts at the FBI have defined insider threats as "authorized users who do unauthorized things for malicious purposes" (Chickowski, March 1, 2013). The insider is a trusted person who may have been loyal and honest for some time and then is recruited by another country or agency to betray his country. Such betrayals are usually due to one or more of three reasons:

(1) There is a change in the individual's values or goals;

(2) There is a perceived breach of trust between the insider and the agency or country involved which causes alienation and justifies the disloyalty in the mind of the subject;

(3) the insider may have been deceptive in his or her intentions from the onset and this was not detected.[2]

The detection of a betrayal by an individual requires an individual-based analysis. The risk assessment requires relevant risk indicators and approaches that can ascertain the values, attitudes, belief systems, ideologies, grievances, friendships, associations, vulnerabilities, intentions and capacities of the individual in question. As the FBI has noted, it is a person-centric problem. It is also important to understand the risk indicators that are present. A comprehensive risk assessment approach should contain both risk promoting and potential risk mitigating elements, in order to be able to take action and try to mitigate this risk. The risk decision is then determined after considering both types of information and all the independent risk variables.

The perpetrators of insider criminal offences are often highly educated and skilled. They frequently hold responsible positions. They usually have normal cognitive function and volitional control of their actions. Such

[2] Personal communication: FBI supervisory special agent on March 3, 2014.

individuals are capable of making rational decisions and changing the nature of their actions over time based on what they consider to be new compelling reasons. As a result, the risk indicators for insider threat have a dynamic component. This differs from tools that use static risk indicators such as sex, age, education, criminal history, childhood abuse and uncontrolled urges and impulsive actions. The presence of mental illnesses should be considered in a risk assessment, but this should be mostly for purposes of screening out of mentally ill employees. For purposes of the risk assessment protocols considered in this document for "insider threat", "insiders" are considered to be inherently "normal "functioning individuals who have chosen to act disloyally or violently, not out of mental illness or compulsions, but as a volitional and rational decision based on identifiable motivations.

Insiders are known to have engaged in espionage, sabotage or other treacherous and treasonous acts out of the lure of money, sex, blackmail, emotional trauma and ideological reasons. Expert reviews of the literature related to multiple cases of insider deception and betrayals have revealed that in almost all cases, the compromised individual exhibited identifiable signs. These signs went unreported for years due to what has been called the unwillingness of colleagues to accept the possibility of treasonous action by their friends or colleagues (*The Insider Threat*). Described in military terms, the adversary who makes a frontal attack is easier to anticipate or turn back with countervailing force than an adversary who attacks from within because this individual is "not so readily anticipated nor defeated by force alone" (Catrantzos, September 2009). Because the adversary is so difficult to anticipate, risk assessments of such individuals are no easy or certain task.

Required Elements for Risk Assessment of Insider Threat

The above suggests that an individual risk assessment for high security clearance should include the following characteristics:

(1) an exploration of relevant attitudes in a robust manner to identify potential deception;

(2) maintenance of an ongoing and regular sequence of dynamic reviews of those engaged in sensitive positions to permit the early identification of dynamic changes in situation or values that could affect loyalty, and

(3) monitoring of status of the individual relative to the organization including disgruntlement, lack of anticipated progress within the organization or other disillusionment with the agency that could be interpreted as breach of trust by the insider.

Individual risk assessments require vigor and comprehensiveness. Criminal background checks, credit reviews, financial status and educational background verification, while useful for selected elements of reliability do not address loyalty issues nor the values and ideologies held by an individual. They also do not account for the dynamic changes that may occur over time in terms of risk elements. Insider risk assessment, by its nature, is multi-dimensional and involves many factors. It is a complex problem and it requires a correspondingly complex analysis of the drivers motivating an individual, an exploration of the moral emotions, attitudes, values, personality characteristics other psycho-social elements and an examination of the associations of the individual. As all crime can be related to motivations that are personal, social, political or economic, so can insider threat be so attributed.

Proactive steps are necessary to detect and mitigate risks that exist before asthey mature into dangerous actions. These proactive steps require the development and implementation of countering insider threat strategies (CIT- strategies). The most fundamental of these is a comprehensive and perceptive risk assessment. The assessment can be followed by a sensitive and targeted intervention to mitigate this risk. This intervention is individualized and objectives can be identified from a distinctive features analysis of the generated risk assessment.[3] The military is particularly vulnerable to catastrophic consequences of insider attacks. This potential for devastating damage is due to the advanced weaponry training of insiders, their ability to strategically plan attacks and their capacity use military assets effectively. Other insiders are in a position to disclose national security secrets. A literature that examines individuals who have perpetrated unlawful and serious insider offences can provide valuable insight into the risk indicators to be included in a sensitive and appropriate risk assessment protocol. Due to purposes of space, only three such examples are presented below.

Insider Case Studies and Lessons Learned

The Insider who Represents a Risk. "Trusted persons" who have access to facilities or assets may not engage in acts of sabotage, espionage nor be perpetrators of violent attacks, but they may permit access to others who do have malicious intent. The individual providing the access may not have

[3] This is a basic clinical assessment model, specifically identification of problems through structured analysis and then targeted intervention to address the identified issues.

malicious intent. Similarly, an unlawful act of disclosing classified information may be unintentional rather than intentional and malicious.

Whether intentional or unintentional, malicious or non-malicious, the act itself is unlawful and the actor is subject to penalty. This was recently demonstrated. On February 7, 2014, Stephen Jin Woo Kim, age 46, was prosecuted for leaking information to the media. He entered a guilty plea and was sentenced to 13 months in prison (Ingram, 7 februarie 2014). Kim is one of only 11 cases in United States history where an individual was prosecuted for an unintended act of leaking information. Kim claimed he had no malicious intent. He did admit to "letting his guard down" which caused a lapse in his conduct.

Kim was a highly respected State Department contractor when he was arrested. He was a deeply embedded "insider" having worked for the Centre for Naval Analysis and the Defense Policy Board. He had been an advisor to both Henry Kissinger and Dick Cheney on issues related to his expertise. He had worked for the Under Secretary of Defense (*Wall Street Journal*, February 7, 2014).

Canada, like the United States and other nations, is not immune to insider threats. One year earlier than the Kim case, Jeffrey Delisle, as identified earlier, was convicted and sentenced to 20 years in prison in February 2013, for selling secrets to the Russians. Patrick Curran, the Chief Judge of the Nova Scotia Provincial Court, commented that Delislehad acted "coldly and rationally" beginning in 2007 (*Globe and Mail*, February 8, 2013). Delisle confessed to betraying his country by providing information from top secret-level computer networks to Russian agents for five years. He had been "risk assessed". In these assessments, he was judged by the officials responsible for this evaluation to be loyal and trustworthy. He had top level security clearance and his position included access to highly sensitive information as an intelligence analyst.

Such risk assessment sare time and situation dependent. Delisle is an example of an individual assessed at one point as reliable and trustworthy and who may have been so at this time but who was clearly not equally reliable and trustworthy at a later time point. Circumstances and behaviors of individuals change as had occurred with Delisle. He made a rational and volitional decision to betray his country.

Individual risk assessments for high level clearance personnel should be undertaken on a frequent and regular basis. The assessment should be standardized to enable a comparison of results at different time intervals. Although such repeated measures are time and human resource intensive, ongoing monitoring at regular intervals is essential if risk assessments are to be reliable. Although individual assessments of risk may not always deviate over time, any generalization as to the consistency of loyalty and trustworthiness is reckless and imprudent, as well as potentially dangerous. The first risk assessment undertaken will generate baseline data from which other assessments can be compared. The use of quantifiable reliable measures will highlight observed changes. The application of a structured and objective professional judgment of risk will provide continuity.

It is vital that risk assessment protocols use pertinent risk indicators. These indicators include personality, psycho-social factors, values and ideology, political issues of concern, grievances both political and social and economic circumstances. Information on these points of interest are often provided as information lists to assessors rather than as a structured coherent tool that can be administered.

There are important lessons to be learned from a literature review of Canadian and international cases of insiders who have inflicted damage to the security and intelligence capabilities of their nations. These lessons can be summarized as follows:

(1) a requirement exists for a robust individual risk assessment protocol for insider threat;

(2) the protocol should be systematic, criterion based referenced and use an accepted behavioral methodology;

(3) a set of pertinent and comprehensive risk indicators are required;

(4) the risk assessment should be undertaken at regular time intervals and the results that are produced through the reliable methodology for an insider should be compared over the time line used;

(5) in addition to the formal protocol, it is important to obtain as much information as possible on the "insiders", including accessing informal observations, reports, intelligence information, information on personal motivations, values and other accessible information for use during the formal risk assessment protocol.

These recommendations are consistent with FBI insider threat experts who have identified behavioral approaches to risk assessment of insiders as the most promising of all options to identify and mitigate insider threats and who support a person focused multi-dimensional risk assessment for "insiders" (Chickowski, March 1, 2013). Many insiders who have betrayed their countries were active for years before they were identified and arrested. With the current status of computerization and network access to secrets, huge amounts of sensitive information can be obtained from agencies in a shorter time than ever before. This information can be extracted from the computer networks and removed on portable memory drives with relative ease. The Office of the U.S Counterintelligence Executive noted that the amount of information lost through relatively recent insider threat constitutes more than the sum total of what was previously "given to our enemies throughout U.S. history" (*Insider Threat*).

Recent and serious insider betrayals have supported the urgency for improved security protocols and the use of new and more objective tools to permit detection of insider threats. The major objective of risk assessment is to identify potential risks in order to initiate preventative action to mitigate risk. Most government installations are improving physical security procedures, increasing cyber security and making technical improvements. The added application of new and improved behavioral analysis and individual risk assessment tools will further enhance comprehensive insider threat security provisions.

Case Examples: Espionage, Sabotage, Violence, Unauthorized Disclosure

Case Example 1: Jeffrey Paul Delisle: Navy Insider Espionage. Jeffrey Paul Delisle, a former Sub-Lieutenant in the Royal Canadian Navy, wasin a post at the Trinity Naval Intelligence Fusion- Centre in Halifax, Nova Scotia when he was arrested on charges of espionage which had been ongoing for five years. He had access to the "Stone Ghost" intelligence sharing network database of the Five Eyes used having received "Top Secret Five-Eyes Only" clearance. He passed sensitive information from this network to the GRU, the intelligence branch of the Russian Armed Services. Delisle had walked into the Russian Embassy in Ottawa in July 2007 to volunteer his services. Much of the information passed to the GRU was U.K., U.S. and Australian intelligence information. For Canadian Military Intelligence, he used "SPARTAN", a Department of National Defence network and he was thought to have provided Canadian civilian intelligence reports from CSIS, the RCMP, the PCO, Transport Canada and the Canadian Border Service Agency (CBSA).

Delisle, who was a naval intelligence officer and threat assessment analyst is quoted as saying after his arrest that "we spy on everybody, everybody spies". This was the explanation provided by him for giving the Russians sensitive materials. ``I tried to just give them [the Russians] stuff that shows them that `Hey, we're just paying attention.' (*RCMP full interview with Jeffrey Delisle*)''. He said that much of the information he passed on was from SIGINT (signals intelligence) and not from human sources.

Under interrogation, Delisle admitted passing Russia the information on material originating from Canada, Britain, the United States and Australia. He sent over conversations obtained from electronic surveillance, as well as "contact lists" of intelligence officials. He denied ever giving up undercover spies. At a court in October 2012, Delisle pleaded guilty to breach of trust and two counts of passing secret information to a foreign entity contrary to the Canadian Security of Information Act. On February 8, 2013 he was sentenced to 20 years in penitentiary, minus time already served.

There are lessons to be learned from Delisle's case. First, there should be ongoing assessments and monitoring of the attitudes of those having top secret clearance on an ongoing basis. This should be undertaken from an established baseline at time of onset of the clearance. Delisle's views on SIGINT information became problematic later in time and he is thought to also have become discontented with his position. Second, it is essential to monitor the personal context of those with high clearance to determine the changing vulnerabilities caused by marital, financial, other problems. This was a factor with Delisle. Third, it is necessary to observe and assess the personal characteristics of top clearance personnel to determine personality and behavioral characteristics such as narcissism, lack of compliance with rules, gaming and other addictions. Delisle reported to interrogators that he acted due to the emotional stress caused by the breakdown of his marriage and his wife's affair. Other elements such as his personal views are considered to have contributed to his betrayal decision.

Case Example 2: Robert Philip Hanssen-Insider (FBI) Espionage. Robert Philip Hanssen is a recent and serious case of insider espionage in the United States. Like Jeffrey Delisle, who was discussed previously, Hanssen, who was a FBI Special Agent, was providing significant amounts of sensitive information to the Russians. At the time of his arrest at a park in Vienna, Virginia in 2001, Hanssen was clandestinely placing a package containing highly classified information at a pre-arranged, or "dead drop" site for pick-up by his Russian handlers. Money was the apparent motive and Hanssen had previously received substantial sums of money from the Russians (FBI Press Release on Robert Philip Hanssen case, February 20, 2001).

FBI Director Louis J. Freeh described Hanssen's action as representing "the most serious violations of law and threat to national security" and that insiders in the military and civilian police are guilty of especially egregious"-betrayals of trust" because they are agents sworn to enforce the law and to protect our nation's security. Hanssen minimized his action stating on his arrest that "I could have been a devastating spy, I think, but I didn't want to be a devastating spy. I wanted to get a little money and to get out of it" (FBI Press Release on Robert Philip Hanssen case, February 20, 2001).

Hanssen was charged and entered a guilty plea to espionage and conspiracy to commit espionage. In 2001 he was sentenced to life in prison without the possibility of parole. The criminal affidavit against Hanssen provided an account of how he first volunteered to furnish highly sensitive documents to KGB intelligence officers assigned to the Soviet embassy in Washington, D.C. He also chronicled the systematic transfer of highly classified national security and counterintelligence information in exchange for diamonds and cash worth more than $600,000 (estimated by other sources to be in the range of $1.4 million).

Hanssen clandestinely left packages for the KGB, and its successor agency, the SVR, at dead drop sites in the Washington area on at least 20 occasions, and caused significant damage by providing the KGB/SVR with over two dozen computer diskettes containing disclosures of over 6,000 pages of important material. He compromised numerous human sources of the U.S. intelligence community and provided Russia with dozens of classified U.S. Government documents, including "Top Secret" and "codeword" documents. He also provided information on what has been described as technical operations of extraordinary importance and value

Hanssen, similar to insiders like Delisle, had direct and legitimate access to voluminous information about sensitive programs and operations. He used his training, expertise and experience as a counterintelligence agent to avoid detection. He kept his identity and place of employment from his Russian handlers and avoided the customary "tradecraft" and travel usually associated with espionage. He was not detected by inside risk assessment, but as a result of other outside information that had been obtained by the government.

Case Example 3: David Sheldon Boon: Army Insider Espionage. David Sheldon Boon joined the U.S. Army when he was 18 years of age and remained in the military for over 20 years until he retired in 1991. He worked as a Signals Intelligence (SIGINT) Analyst of foreign communications. He also produced combat, strategic, and tactical intelligence reports. He had studied Russian at the Army's Defense Language Institute in Monterey, California and in 1985 was assigned as a senior cryptologic traffic analyst to the NSA at Fort Meade. In this position, which he held for three years, he had access to sensitive information about the capabilities and movements of Soviet forces and Soviet tactical nuclear weapons and he produced reports on Soviet Fire Support Operations. He was assigned to a US field station in Germany, Europe, but before his transfer, he made the decision to become a spy for the Soviet Union and walked into the Soviet Embassy in Washington, D.C. and volunteered to sell classified military documents for cash[4].

Boone made the decision to betray his country in 1988 before he was sent to Germany. His marriage was broken down, he was financially struggling with support payments to his wife and children, he was angry over the "fair' rating received on his NSA performance evaluation and he was irritated at the U.S. legal system and the outcome in his divorce case, which put financial pressure on him. Boone admitted that "I needed money. Plus, well, I was extremely angry".

For between 3 and 7 years until Boone lost his security clearance, he was engaged in espionage activities with a Soviet handler who met with him several times a year. He received payments totaling estimated at more than $60,000. His periodic re-investigation for his security clearance revealed Boone's financial problems and debts and in 1990, his access to classified information was suspended when he lost his top secret clearance due to lack of personal and professional responsibility. He was reassigned to serve at a military hospital where he remained until his retirement in 1991, which put an end to his espionage career and relationship with the KGB. In 1998, Boone was contacted by an undercover FBI officer posing as an agent of the SVR (Russian successor to the KGB) who wanted to re-activate him due to some event that triggered an investigation of him.

Boone traveled to London for two meetings with his "handler" while he was being recorded. He recounted in the meetings in detail how he had volunteered his services to the KGB, and how he had passed highly classified and extremely sensitive national defense information to the Russians over a period of three years. Boone then agreed to resume spying and work with the SVR and accepted a payment of $9,000. Next, he was lured to the U.S. for another meeting with his handler where, on October 10, 1998, he was arrested at the Washington Dulles International Marriott Hotel in Reston, Virginia.

[4] Hardcopy from US Attorney's Office, Eastern District of Virginia; regarding David Sheldon Boone dated October 15, 1998 See related court docket: http://jya.com/dsb101498.htm*The Affidavit in Support of Criminal Complaint,Arrest, Warrant, and Search Warrantsfor David Sheldon Boon* provides comprehensive information from the FBI on this case. Available at http://cryptome.org/jya/dsb100998.htm Retrieved March 27, 2014. Information is also available from Department of Energy, Hartford on Boon at the following site http://www.hanford.gov/c.cfm/oci/ci_spy.cfm?dossier=170RetrievedMarch 24, 2014.

Boone was charged with espionage, entered a guilty plea to conspiracy as part of a plea bargain, forfeited $52,000 including his retirement fund and submitted a hand-held scanner he used to copy documents. On February 26, 1999, he was sentenced to over 24 years in prison (Davis, 1999).

Case Example 4: Theresa Squillacote-Pentagon Insider Espionage. Theresa Marie Squillacote, age 42, a Pentagon lawyer, was arrested and charged with spying for East Germany and Russia on October 4, 1997. She was arrested with her husband Kurt Stand, age 45, who was a left-wing labor activist and James Michael Clark, who was a private investigator. Clark entered a plea of guilty and was a prosecution witness against Squillacote and Kurt Strand. All three had been active in the Communist Party's Youth Movement at the University of Wisconsin in the 1970's. Squillacote and her husband were convicted in October 1998 of conspiracy to commit espionage, attempted espionage and related charges having relation to classified documents. Squillacote was sentenced in January 1999 to 21 years and 10 months and Kurt Stand was sentenced to 17 years and 6 months (*CBS news*).

Squillacote had graduated from Catholic Law School in Washington, D.C. and obtained a job at the National Labor relations Board, followed by the House Armed Services Committee as a staff attorney and finally a position at the Pentagon. It is believed that Squillacote's husband began his espionage activities in approximately 1972 and he recruited her approximately in 1980 when they were married. The espionage activities of Squillacote and the others were documented in STASI files obtained by the CIA after East Germany's collapse and after five years of inter-agency fighting, finally were released to the FBI. After the collapse of the Soviet Bloc, in June 1996, Squillacote sent a letter to a South African Official and Communist Party leader indicating that she had no admiration for bourgeois parliamentary democracy and suggested a working relationship. The letter was forwarded to the FBI. Squillacote was subsequently caught in an FBI sting operation in which she passed sensitive Defense Department documents to an undercover FBI agent. Her former associate Clarke testified against her that he had passed documents to an East German spy, Lothar Ziemer with whom Squillacote and Stand were alleged to have worked. The case and especially Squillacote did not receive much attention, but it has generated some controversy because of the nature of the evidence and the sting operation.

The case does underscore the need for relevant risk assessments which differentiate the "freedom" one has under the laws of a State to hold a political viewpoint that departs from the norm, from an assessment of the risk which holding these views might represent in some circumstances and positions. A security clearance at a high level should assess this risk despite the freedoms and protections that exist to hold them. It also identifies the potential role of psycho-social factors in risk assessment[5].

Squillacote was a senior procurement analyst in the Office of the Deputy Under-Secretary of Defence for Acquisition Reform and had high-level clearances until she was arrested. She had never concealed her political views or her associations. She married the son of an open and active Communist. She traveled regularly through the Soviet Bloc. She named her children after German Communist "martyrs". Despite this history and her views she was able to secure a post as a staff attorney in the House Armed Services Committee during the Cold War and went on to work in the Pentagon after receiving a higher security clearance level. Squillacote is reported to have told an undercover FBI agent that she "turned to spying to support the progressive anti-imperialist movement". Squillacote's action was "Defence Department Insider Espionage". This case reflects an ideological motive with the potential involvement of psychological vulnerability.

Case Example 5: Nidal Hasan: Army Insider Violent Acts (Terrorism/Violent Extremism). On November 5, 2009 at 1:34 p.m., Nidal Malik Hasan, an American citizen and United States Army Medical Corps Officer, walked into the Soldier Readiness Center of Fort Hood in Killeen Texas, and fatally shot 13 people and injured 32 others. He used a semi-automatic Five-Seven pistol. Hasan was born in Arlington, Virginia September 8 1970, was 39 years old and was a United States Army psychiatrist. He readily admitted to the killings. There was controversy as to whether Hasan's act which was ideologically motivated was an act of "terrorism", or "workplace violence". He was tried on 13 counts of pre-meditated murder and 32 counts of attempted murder and convicted by a panel of 13 military officers on all counts (*A Ticking Time Bomb*, February 2011).

Investigators in the FBI and U.S. Army have determined that Hasan acted alone. His trial was delayed for a variety of procedural and representational issues. On June 3, 2013, a military judge allowed Hasan to represent himself at his murder trial. During the first day of the trial on August 6, 2013, Hasan admitted that he was the gunman during the Fort

[5] See a discussion in the American Psychological Association Monitor of the monitoring of conversations between Squillacote and her psychotherapist and the role of psychological profiling. Retrieved March 28, 2014. http://www.apa.org/monitor/julaug02/jn.aspx.

Hood shootings. He also told the panel hearing that he had "switched sides" and regarded himself as a Mujahedeen waging "jihad" against the United States. He justified his actions by claiming that the US military was at war with Islam. Hasan had communicated to medical health experts assessing him in 2010 that he "would still be a martyr" if convicted and executed by the US government. Hasan did not call any witnesses in his trial consistent with his admission and strong ideological position that his action was justified. He was sentenced to the death penalty on 28 August, 2013. The sentence is under appeal.

Hasan was the child of Palestinians who immigrated to the US from the West Bank. He joined the United States Army after high school graduation in 1988 and served eight years as an enlisted soldier while attending college. He graduated from Virginia Tech in 1997 with a Bachelor's degree in biochemistry and then studied medicine at the Uniformed Services University of the Health Sciences (USUHS), graduating in 2003. He followed this training with an internship and then a residency in psychiatry at the Walter Reed Army Medical Centre and obtained his psychiatry accreditation in 2007. This was followed by a further Master's Degree in Public Health at USUHS with a two-year fellowship in Disaster and Preventive Psychiatry at the Center for Traumatic Stress at USUHS. He completed this training in 2009. He was promoted the same year from captain to major.

There have been several government investigations into the Fort Hood Insider shooting. These have identified missed red flags in Hasan's case. The most salient question in relation to insider threat assessment highlighted by this case was the evident failure to identify the risk that Nidal Hasan represented. Either incorrect risk indicators were used in the risk assessment for Hasan for violent extremism, or no formalized and comprehensive risk assessment was undertaken. Many risk indicators relevant to the risk of violent extremism were present.

The risk indicators in the VERA 2 (Violent Extremism Risk Assessment-Revised Version) can be explored in terms of their relevance to Nidal Hasan and the information that they would have been able to provide to assist the identification of potential insider threat. To be considered a significant risk (moderate to high) level for violent extremism, all of the risk indicators in the tool do not need to be documented as present and evaluated at a high level. All of the indicators are considered and rated if information is available, and if information is missing, this identifies information to attempt to obtain for assessment. The final risk judgment is not determined by an additive method. It is determined by professional judgment that assisted by the use of a structured and systematic methodology applying the comprehensive set of risk indicators for violent extremism (in this case). Each risk indicator is evaluated on the basis of pre-established and quantifiable criteria and a risk level for each of the indicators individually is obtained. Following this comprehensive indicator by indicator analysis, the information collected and structured with the ratings produced are reviewed and analyzed. An objective and reliable risk decision is determined following this analysis and review. The presence of a limited number of significant risk indicators assessed at a moderate to high level on the VERA 2 (Risk Assessment of Violent Extremism) is sufficient to arrive at a risk assessment that identifies serious concern as to the danger or potential hazard posed by the individual. In the case of Nidal Hasan, the red flags were present.

The VERA 2 indicators that would have clearly documented insider danger are listed and described below. The evidence for the analysis below is available in the report on the Fort Hood Shooting undertaken by the U.S. Senate Committee on Homeland Security and Governmental Affairs and released in February 2011 (*A Ticking Time Bomb*).

Risk Indicator 1: Victim of injustice and grievances. Hasan's grievances were often stated publically by him to colleagues and supervisors. They related to the U.S. position, the U.S. military deployment in Muslim lands (Afghanistan and Iraq) and he saw the U.S. position as a war against Islam. He also had expressed his grievance against his supervisors in the U.S. Military who did not react to his complaints concerning the actions of men he was treating and who had returned from Afghanistan. He thought their actions that they had discussed with him in clinical sessions should have been considered war crimes.

Risk Indicator 2: Identification of the person, place, or group responsible for the injustice or grievance. Hasan had openly identified the source of his grievances which was the U.S. Military. He made critical remarks to colleagues as evidence of this viewpoint and was known to have made anti-American remarks in his lectures prior to the shooting. Some of these remarks were reported to supervisors. Val Finnell, a former medical school classmate is reported to have complained to superiors about Hasan's "anti-American rants". He commented that the "system" was not doing what it was supposed to do and that Hasan should have been confronted about his anti-American views (Passatino and Winter, November 10, 2009).

Risk indicator 3: Commitment to an ideology justifying violence based on a higher authority rather than the jurisprudence of the nation. Although Hasan was disciplined for proselytizing about his Muslim faith with patients and colleagues in his third year at the Uniformed Services University of the Health Sciences (USUHS), particularly significant as a risk indicator of a high level was the nature of his attitudes and beliefs. He was unable to differentiate his professional and political views and his ideological position was observed to be the primary driver of his worldview much before the attack on November 5, 2009. Hasan was required to give medical lectures as part of his responsibilities. Students and colleagues attending these presentations expected them to be related to medical issues, but they were often a denunciation of infidels.

It had been documented in a slide presentation to U.S. Army Physicians at the Walter Reed Army Medical Centre during his senior year of Psychiatric residency that his views were in opposition to those of the U.S. government and the U.S. military. Specifically, one presentation entitled "*The Quranic World View As It Relates to Muslims in the U.S. Military"* specified elements of his attitudes and ideology. This was a missed red flag. Slide 49/50 of this presentation asserted that "*God expects full loyalty*", that "*God is not compromising"* and that "fighting to establish an Islamic State to please God, even by force, is condoned by Islam". Further Hasan asserted that Muslim soldiers should not serve in any capacity that renders them at risk to hurting or killing believers in Islam.

This presentation could reasonably have been interpreted to suggest that:

(1) Hasan's primary loyalty was to God rather than to the U.S. military or the United States;

(2) that Hasan believed that the Taliban were correct and morally justified in fighting for an Islamic State in Afghanistan;

(3) that the use of force by "America's enemy" in Afghanistan is religiously sanctioned by God;

(4) that American Muslims cannot fight in any Muslim land due to the risk of hurting or killing other Muslims, even on the battle field. This ideology, supported by behavioral evidence, puts Hasan in direct conflict and opposition to U.S. policy. It also puts him in conflict with legally sanctioned military action taken by the United States.

At a minimum, these indicators required serious exploration in a comprehensive risk assessment protocol. Hasan, as a citizen, had the rights and freedoms to hold his religious beliefs, but as Dr. Finnell has pointed out, when you are in the military you have sworn to defend your country from its identified enemies. Finnell recalled Hasan telling classmates and professors that "I'm a Muslim first and I hold the Shariah, the Islamic Law, before the United States Constitution"(Passatino and Winter, November 10, 2009).

Risk Indicator 4: Personal Contact with Violent Extremists: BetweenDecember 2008 and June 2009, Hasan was known to be in personal contact with Anwar al-Awlaki, who was a violent extremist. As a single risk indicator noted, this would be considered extremely significant in terms of weighing potential risk. Hasan was known by the U.S. government to be in email contact with al-Awlaki, a virulent anti-American ideologue on 18-20 occasions. Al-Awlaki (now deceased as a result of an American attack) was an influential and charismatic promoter of "jihad" attacks in the United States, and a known and prominent Al-Qaeda recruiter. Hasan was investigated by the FBI after U.S. intelligence analysts intercepted the e-mails between him and Anwar al-Awlaki. Al-Awlaki praised the Fort Hood attack and is quoted as reporting that rather than convincing Hasan to engage in violence, Hasan was providing justification to him. It has been reported that U.S. investigators were aware that Hasan had also attempted to contact Al Qaeda and that he had other "unexplained connections to people being tracked by the FBI" in addition to Anwar al-Awlaki (Raddatz, Ross, Abraham and El-Buri, November 10, 2009). These are serious risk indicators.

The assessment by the D.C. Joint Task Force was that the emails and other material did not call for a larger investigation. Defense Department officials said they were not notified of these investigations before the shootings (Raddatz, Ross, Abraham and El-Buri, November 10, 2009). It is difficult to comprehend how a decision for no follow-up was reached considering the importance of this risk indicator alone for potential acts of violent extremism. The dynamic nature of the radicalization process could have justified ongoing monitoring. As former CIA officer Bruce Riedel has stated "emailing a known al-Qaeda sympathizer should have set off alarm bells" and "even if he was exchanging recipes, the bureau should have put out an alert"(Examiner, 2002).

Risk Indicator 5: Seeker, Consumer of Violent Extremist Materials It is known that Hasan was visiting radical Islamist websites. Although the full extent of this cyber behaviour was determined after Hasan's computer was examined which occurred after the shootings, any investigation based on the previous risk indicators would have uncovered these internet searches and Hasan's cyber behavior before the attack.

Risk Indicator 6: Feelings of Persecution, Alienation, and Isolation Hasan had been described by colleagues as withdrawn, socially isolated and stressed by his work. This stress was augmented by his work with returning soldiers. There is some suggestion that Hasan may have felt some religious harassment in the military and that he became alienated. He was considered to be unassuming, brooding and socially awkward (*A Ticking Time Bomb*, February 2011). He was never known to have had a girlfriend. After the fatal shooting of two recruiters at the Army recruiting centre in Little Rock, Arkansas by Abdulhakim Mujahid Muhammad, who later claimed to be an Al Qaeda terrorist, Hasan was described as upset that the perpetrator was being charged with murder.

Risk Indicator 7: Early Exposure to Pro-Violence Militant Ideology. It is known that Hasan came from a Palestinian family that had left the West Bank area when they immigrated to the United States. Although the family's immigration was prior to Nidal Hasan's birth and he appeared to have led a normal American life, the views of his family members, associates and others with whom he may have been in contact during his childhood and youth should have been explored in a risk assessment. This exploration would have included those suggesting the legitimacy of militant action against the U.S. and other states that supported perceived anti-Muslim policies or the State of Israel. A risk assessment of Hasan should also have highlighted his prior exposure to al-Awlaki at the Dar al Hijrah Mosque in Northern Virginia where al-Awlaki was the Iman from January 2001 to April 2002. Hasan may have been influenced at a vulnerable time by al-Awlaki after his Mother's death or by "incipient radicalization" in his youth which progressed as he matured.

Risk Indicator 8: Willingness to die for Cause or Martyrdom. The willingness to consider the act of martyrdom or dying for one cause is an important risk indicator for violent extremism. This indicator also explores "suicide bombing" in terms of the subject's views of engaging in such an act. Elements pertaining to one's potential willingness to engage in or justify acts of martyrdom are also explored in this indicator. In theemails intercepted by U.S. officials from Hasan to Al-Awlaki, Hasan apparently wrote that "I can't wait to join you in the afterlife" and he asked al-Awlaki when *jihad* is appropriate, and whether it is permissible if innocents are killed in a suicide attack. One specific email was known to be particularly problematic in terms of the justification of suicide bombing and martyrdom. In the months before the shooting, Hasan is known to have increased his contacts with al-Awlaki which itself would raise red flags about Hasan and would support the behavioral evidence of a dangerous change in risk level. Hasan,during his trial in his trial, was open about his view that he will be be a martyr even if executed by the U.S. government.

Risk Indicator 9: Glorification of Violent Action. Hasan had come to the attention of federal authorities at least six months before the attacks because of internet postings he appeared to have made discussing suicide bombings and other threats (CBS News, November 5, 2009). Authorities had not definitively tied these postings to him although they were made in the name of 'NidalHasan". The postings likened a suicide bomber to a soldier who throws himself on a grenade to save his colleagues, and sacrifices his life for a "more noble cause" and "is an act not despised by Islam but is rather to be considered a strategic victory". No investigation was opened. This indicator relates to the risk element that the subject may be or is motivated by the "glorification of violent action. This ties an action to a perceived noble cause which can be justified or that support a higher authority such as a directive of God.

Risk Indicator 10: Planning and preparing Unlawful Violent Action. Hasan, due to his military training had the capacity to use weapons and to plan and prepare an attack. He also had sufficient resources and organizational skills to plan an attack. This indicator would apply to most "trusted insiders" in the military. As a result, intention is a critical element in the risk analysis of military personnel.

These 10 indicators represent a moderately high to high risk rating for Hasan. They correspond to approximately 50 percent of the included risk indicators in the VERA 2 in addition to indicators exploring the motivational typology and the protective factors. The information available on these identified indicators would have generated enough red flags to identify Hasan as anrelatively high risk as an insider threat to the military prior to the attack. This rating would have ensured closer monitoring of Hasan and may have provided an opportunity for action related to the mitigation of his risk or preventive action. Although there is uncertainty in any risk assessment involving violent extremism, there is valuable systematic baseline information that can be obtained from an objective and transparent protocol. This can not only identify potential risks, but also initiate actions that are aimed at mitigating these risks.

Lessons Learned from Insider Cases

Risk Indicators for estimating "insider threat" can be extracted from an examination of these illustrative cases. The risk elements relate to economic, political, social and personal factors. Economic risk indicators are known to be a powerful motivating driver for many insider betrayals so any risk assessment approach for insider threat must include elements that evaluate the financial situation of subjects. In addition, psycho-social aspects of the financial circumstance should be examined. These are the elements of interaction between the personal, social and economic factors. This can relate to the unmet expectations and wants of an individual in addition to the actual debts and financial status of the individual. In addition, economic factors may be affected by other personal stresses such as divorce, financial demands of children or wives, and vulnerable behaviors (addictions to gambling, alcohol, drugs). Personal risk factors relate to personality factors and include self-importance, narcissism and emotional instability, aggression and alienation. Social factors may relate to grievances related to the social environment such as perceived discrimination due to race, religion, social values or anticipated benefits or social classifications. Political factors relate to the political ideology and attitudes of the subject, the political positions that have been taken by the government, and the legal structures that affect political will.

Risk assessment tools, in order to provide applicable and useful results, must employ indicators that are specifically relevant to the type of risk assessed (Pressman and Flockton, 2012). As a result, it is recommended that a specific tool for risk assessment be developed pertinent to insider threat. This tool will include a comprehensive set of risk indicators identified from the lessons learned from the analysis of known cases. These risk indicators also address criminality in general. The risk indicators will be organized into a structured professional judgment protocol in a like manner to the VERA 2 risk assessment protocol (Pressman and Flockton, 2012), discussed earlier in this paper. However, unlike the VERA 2, the risk indicators will be broader than those related to violent extremism alone.

Risk Assessment Tool Development for of Insider Threat

Conceptual Overview. The lessons learned from the analysis of the various types of insider cases can be applied to the characteristics required for the development of a relevant risk assessment tool. Such a tool would have to apply to all the cases presented above and be sensitive to estimating the risk of individual insiders. The VERA-2, a risk assessment tool for violent extremists will apply to some ideologically motivated insiders who present a threat to agencies. However, none of the indicators in the VERA-2 tool are related to the economic motivations seen in many espionage cases, such as those identified and discussed in the previous section of this report. There are also no indicators in the VERA-2 that are relevant to troublesome and potentially indicative personality indicators such as narcissism, lack of compliance with rules; non-acceptance of the military culture, rejection of military values, job satisfaction; disgruntlement with job advancement and personal vulnerabilities. There are no indicators pertinent to addictions such as drug, gambling or alcohol or other personal problems that require consideration in insider threat. It is advisable, therefore, that a risk assessment tool be developed specifically pertinent to the unlawful insider betrayals. The VERA-2 should be used in cases where ideological motivation is present and there are potential risks for violent extremism. In other cases of insider threat, the risk assessment of individuals should be undertaken with the tool developed for this purpose. Such a tool was developed for this purpose and is presented here. Details of the tool's user guidelines are available from the author. This tool, referred to as the RAIT (Risk Assessment for Insider Threat) will include the elements identified from the literature and case study reviews. The specific indicators are identified below. Specific rating guidelines are available under separate cover.

The Risk Assessment Tool for Insider Threat (RAIT). The RAIT tool is a structured professional judgment tool that uses the same systematic and reliable methodology as used in the VERA-2 risk assessment protocol. Reports from users of the VERA-2 have reported that this consistent and systematic methodology has been beneficial for security and intelligence applications. Reports from professionals on four continents over the past five years (including police, intelligence analysts, psychologists, psychiatrists and lawyers have supported the efficacy and relevance of this tool.) The RAIT uses the same behavioral method, but include specifically pertinent risk indicators for insider threat.

The RAIT uses 25 discrete risk indicators, each of which will be rated on a 3 point scale (extendable to a 5 point scale). The risk indicators are divided into four categories that are appropriate to unlawful insider action drivers. These are (1) political, (2) social, (3) economic and (4) personal motivations. In some cases, the actor may be motivated by more than one of these elements. According to FBI expert opinion, these four motivations account for the motivations of all criminal acts.[6]

The risk indicators extracted from the literature on insider threat and from the analysis undertaken on known cases were organized into a structured professional judgment (SPJ) protocol in a manner consistent with other SPJ tools. Criterion-based ratings for each of the risk indicators are consulted to establish a risk levels for each of the indicators. The risk factors are intended to be comprehensive. They apply to insiders engaged in

[6] This model of criminal motivation is based on personal discussion and collaboration with an FBI expert in insider threat at the FBI Critical Incidents Response Group and the FBI Academy at Quantico, VA.

espionage, sabotage, unauthorized disclosure, violent extremism, theft and other insider offences. The indicators incorporate risk and risk mitigating elements. A preliminary RAIT manual with user instructions is available from the author.

RAIT Consultative Risk Assessment Indicators (N=25)

A. POLITICAL FACTORS –ATTITUDES AND VALUES

A1. Political/ideological/religious causes have priority over national laws and military

A2. Perceives political injustice at home and/or abroad, other perceived grievances

A3. Rejects selective societal values

A4. Identity conflict related to political views and military values

A5. Anger at political decisions and actions of country/military

A6. Family living abroad in non-democratic/conflict zone areas

S. SOCIAL FACTORS

S1. Perceives self, group as victim of social injustice

S2. Believes specific race, religion, culture superior to all others

S3. Personal contact with extremists, unlawful violent actors (gang members, criminals)

S4. Prior criminal history/violence

S5. Prior paramilitary training, experience with weapons

S6. Lack of compliance with social/cultural code, military rules

P. PERSONAL FACTORS AND BEHAVIOR

P.1 Exhibits personal aggression, hostility, moral anger

P.2 Exhibits narcissism, self-importance

P.3 Under personal stress (divorce, conflicts, children)

P.4 Unhappy in job assignment

P.5 Exhibits mental instability, personality problems, behavioral disorders

P.6 Frustrations in personal life (relationships, friendships)

E. ECONOMIC FACTORS AND FINANCIAL GAIN

E1. Financial expectations unsatisfied in career

E2. Disgruntled with career advancement

E3. Financial problems

E4.Specific Addictions: gambling, alcohol, drugs, sex

M. MITIGATING-PROTECTIVE ITEMS

M.1 Compliance, participation counseling for personal stress, financial issues

M.2 Courses taken to support career advancement

M.3 Modification of views and grievances, more flexibility in attitudes

Each of these indicators is rated by a criterion-referenced definitional guide and an overall risk judgment is made. This judgment may recommend additional monitoring, interviews, follow-up or intervention.

Conclusions

Insider threat is ubiquitous. Identifying this risk is difficult and replete with challenges. This is in part due to the intentional deception of the perpetrator and the normal characteristics of the agent. Trusted agents in security and intelligence sensitive positions can and do change over time in the potential risk they represent. Insiders who are fiercely loyal at one time may choose to betray in another time period. Such betrayers of government, military or other organizations can cause significant and potentially catastrophic physical, human, economic or national security damage. The insider threat that an individual can pose is dynamic. It is contingent on one or a combination of political, economic, social and personal elements, attitudes and circumstances. For insider threat can be identified and constructed into a tool whereby each of the indicators can be assessed in a standardized method and measured in a structured professional judgment methodology. This provides information on the individual indicators or risk, as well as assisting the judgment of the assessor in an overall risk judgment. A tool for this purpose, referred to as the Risk Assessment for Insider Threat (RAIT) has been developed.

References:

1. Bronswill, Jim, Brewster, Murray, (September 19, 2013), *Declassified file list CSIS's worries over 'insider threat' to security*, în The Globe, accesibil la http://www.theglobeandmail.com/news/politics/declassified-file-lists-csiss-worries-over-insider-threat-to-security/article14431288/.
2. Chickowski, Erica, (March 1, 2013), accesibil pe http://www.darkreading.com/insider-threat/5-lessons-from-the-fbi-insider-threat-pr/240149745 Retrieved March 19, 2014
3. *The Insider Threat*, FBI accesibil pe http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.
4. Catrantzos, Nicholas (September 2009), *No Dark Corners. Defending Against Insider Threats to Critical Infrastructure*, Naval Postgraduate School Thesis, Monterey, California, accesibil pe https://www.hsdl.org/?view&did=33503.

5. *FBI declarație de presă despre cazul Robert Philip Hanssen*, (20 februarie 2001), Washington D.C. accesibil pe http://www.fbi.gov/about-us/history/famous-cases/robert-hanssen.
6. CBS News, (October 23, 1998), accesibil pe http://www.cbsnews.com/news/couple-found-guilty-of-spying/.
7. *CBS News*, (November 5, 2009), accesibil pe http://www.cbsnews.com/news/sources-hasan-web-posts-drew-fbi-interest/.
8. Davis, Patricia, (February 27, 1999), *Ex-NSA worker get 24 years for spying*, în The *Washington Post*, accesibil pe http://www.jonathaqnpollard.org/1999/022799.htm.
9. Examiner (2002), accesibil pe http://www.examiner.com/article/cia-on-the-hunt-for-anwar-awlaki-san-diego-jttf-outraged-by-missed-chance-to-get-him-2002.
10. *Globe and Mail* (February 8, 2013), accesibil pe http://www.theglobeandmail.com/news/national/canadian-spy-jeffrey-delisle-gets-20-years-for-selling-secrets-to-russia/article8390425/.
11. Ingram, David, (February 7, 2014), *Update 2-Former U.S. Analyst Pleads Guilty in Leak to Reporter*, accesibil pe http://www.reuters.com/article/2014/02/07/usa-security-kim-idUSL2N0LC1D820140207.
12. Johnston, Roger, (f.a), *Mitigating the Insider Threat*, accesibil pe http://www.ne.anl.gov/capabilities/vat/pdfs/Insider%20Threat%20and%20Other%20Security%20Issues.pdf.
13. MOSID:00161 și MOSID:00214, documente ale Poliției Militare Canadiene accesibile pe http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid161-military-police.page.
14. *O bombă cu ceas*, (February 2011), Raport al Comisiei pentru Securitate Internă și Afaceri Guvernamentale din cadrul SenatuluiStatelor Unite, accesibil pe http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2.
15. Passatino, Jonathan, Winter, Jana, (November 10, 2009), *Raport pe Fox News*, accesibil pe http://www.foxnews.com/story/2009/11/10/fort-hood-suspect-warned-muslim-threat-within-military/.
16. Pressman, D. E., Flockton, J., (2012), *Calibrating risk for violent political extremists: The VERA 2 Structured assessment* in *The British Journal of Forensic Practise*, 14 (4).
17. Pressman, D.E., (2009), *Risk Assessment Decisions for Violent Political Extremism*, Report 2009-02 – Public Safety Canada, accesibil pe http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2009-02-rdv/index-eng.aspx.
18. Raddatz, M., Ross, B., Abraham, M-R, El-Buri, R. (November 10, 2009), *Raport pe ABC News*, accesibil pe http://abcnews.go.com/Blotter/official-nidal-hasan-unexplained-connections/story?id=9048590.

19. *RCMP full interview with Jeffrey Delisle,* accesibil pe https://archive.org/stream/564122-jeffrey-paul-delisle-rcmp-interview/564122-jeffrey-paul-delisle-rcmp-interview_djvu.txt.
20. U.S. Counterintelligence Executive, "Insider Threat" http://www.ncix.gov/issues/ithreat/Retrieved March 24, 2014.
21. *Wall Street Journal*, (February 7, 2014), *Devlin Barrett, Former State Department Contractor Pleads guilty in leak Case*, accesibil pe http://online.wsj.com/news/articles/SB10001424052702304450904579369153970706392.

SECURITY CULTURE AND PUBLIC DIPLOMACY

PUBLIC DIPLOMACY AND INTELLIGENCE – A PRAGMATIC APPROACH TO A SENSITIVE INTERCROSSING

Iulian DICULESCU[*]

Abstract

The approach assumed by this research study concerns namely the praxeological side of public diplomacy, found at the confluence with elements of state power, more specifically with those features characteristic to the Intelligence activity. The conceptual precariousness characterizing the field, both as an academic discipline and an effective instrument of power, is highly emphasized. Thus, the operational contextualization of public diplomacy, an approach enabled by emphasizing the role of information and by synthesizing a perspective specific to the Intelligence area, is an objective to be looked for. As a result, a comparative analysis is done between these two dimensions, with a focus on the fact that they are not completely separated, and there can be many common aspects, some of them transiting from one side to another.

Keywords: public diplomacy, intelligence, contextualization, comparative analysis, ethics

The precariousness of the conceptual umbrella

First steps. Public diplomacy is in its early development period, both as a study field and an academic research, as well as an effective power instrument (Hayden, 2013). However, it is worth mentioning that unlike those who acquire a structured knowledge of this domain, for practitioners, such an aspect does not represent a major drawback, for they are not concerned with theory, or for those interested in a brief perspective only about this new star in the field of diplomacy studies (Melissen, October 2011, p. 2). If we are to consider both dimensions, however, some states, among which the United States of America, are significantly more advanced in this respect than Romania, where it is only within the last few years that for of public diplomacy began to be organized (e.g. FEDP), scholars started writing on the subject (Dima, 2013), or initiatives to develop such field research within university

[*] Romanian Intelligence Service.

departments were launched. All these examples are early steps, yet very necessary and well-timed for our country. Until recently, and this is not something happening in Romania only, public diplomacy was characterized by precise and episodic mutual commitments, various institutional "shortcuts" and "caprices", and, especially, the excessive dependency on the rather unintentional affinities and skills of some decision makers.

The need for an authentic vision. The fragile status of public diplomacy, both as a study discipline and an institutional practice, is highly contrasting with the major expectations regarding its use in managing nowadays challenges. This happens in a context where it has become obvious that neither geography, nor military capabilities can fully justify or cover the security needs. However though, for public diplomacy to be considered a true action tool in the hands of the state, and not just a simple label used for promotion and image reasons, a set of various conditions should be simultaneously accomplished:

1) mapping and encouraging connections among various types of diplomacy, such as public, military, intelligence *diplomacies*;

2) ensuring not only the superficial coordination at top levels of power hierarchies, but an integrated strategic orientation;

3) encouraging the implication and creativity of the private sector;

4) enabling a minimum institutionalization for the entire range of activities;

The fact that among different state structures, as well as at various decision making levels discussions on public diplomacy have become a clear trend is something obvious, however though these "institutional actors" are not very successful in reaching a common or, at least, convergent understanding on this subject. For instance, some actors use public diplomacy strategies to support their policies (CIR, 2001, concerning the war against terror; Gilboa & Muntean, 2014, the relation with the diaspora, etc.); others advocate that a reform of public diplomacy is a necessary thing (Miculescu, 2005), or express their belief that performances of different structures and specialized policies should be measured (CPD, 2010). Moreover, another category is lobbying for sets of priorities – as they call their initiatives – to be implemented through means of public diplomacy. Finally, a few of them argue in favour of a comprehensive communication strategy that would support the values and interests specific to national security.

Elementary questions. This whole mosaic and the relatively disordered variety of approaches indicate that any state intending to use public diplomacy must first answer in a coherent way to some basic questions:

1) Which are the actors and institutions of public diplomacy?
2) How should their efforts be integrated and focused?
3) What means, in operational terms, to be open to the world without compromising security?
4) How should we deal with annoying propaganda campaigns?
5) How should we move from awareness to appropriate action means?
6) What priorities are most relevant in the context of current threats and opportunities?

As we can clearly see, the term "public diplomacy" is now part of a global conversation, become relatively polyphonic after a period of use and dispute among experts. Moreover, it seems to be an umbrella concept for strategic communications, public affairs, international broadcasting, open operations etc. And often, it is difficult to separate them from an analytical point of view: if, for example, a military commander made a press statement circulated by global media, what should this be considered as? Public diplomacy, military diplomacy, international business or the communication of domestic military intelligence operation? Branding, propaganda and perception management? Obviously, in such circumstances, the "name" is part of the struggle to "make sense", that sense that each side is looking for. Naming and labeling do more than simply describing something: they judge and propose valuable insights, establish semantic fields, propose bridges or demarcation lines.

Cross-contextualization

The role of information. Information remains the strategic resource of greatest value in the field of international relations (Eriksson & Giacomello, 2006), an environment shaped by the actors' understanding and action capacity. However though, the technological evolution and emergency of social networks has deeply changed the speed and the way in which information moves and is consumed. A century ago, a diplomat was allowed to prepare an answer to an action or request within days or weeks. The "closed doors" diplomacy was considered the normal practice, and information leaks were rare. There were no video cameras to constantly monitor and allow the assessment of the diplomat's acting.

Nowadays, diplomacy is operating in a radically different environment: although interaction between states is still marked by a minimum code of confidentiality, it is not secret in itself anymore. Modern diplomacy also includes the public dimension (Barston, 2014, p. 1), and what happens in various parts of the world can rapidly become a matter of public/national interest, knowing that most of these situations should be managed through specific means of public diplomacy.

The operational perspective. A quick example regarding the "consumption" of information if terrorist attacks were to happen is that "democratic countries should cut the terrorists' oxygen consisting in the publicity they rely on" (Thatcher, 1985). This means two things: 1) the media is highly important in each terrorist attack; 2) the role that public diplomacy has in preventing and countering the terrorist phenomenon in the short and long run. Basically, beyond the deaths and material losses determined by such an attack, the only long run/significant impact that terrorism would have would be in relation to the society's response; in other words, risk aversion connected to alarming reactions leading to public fear can feed terrorism or, in some cases, even generate it.

If we choose an approach consisting in the praxeology specific to the Intelligence field, it becomes obvious that public diplomacy represents a working tool, something difficult to imagine some time ago. Of course, there are convincing reasons to support the need for "backstage" or "behind the scene" diplomatic negotiations, just as Kissinger (1998, p. 484) was showing in his example of the peace negotiations between the USA and North Vietnam, 1970-1972, when channels for secret dialogue played a key role.

Generally speaking, the actors of this process cannot conduct their activity in complete secrecy, fully separated by the close look of many categories of interested public (partners, beneficiaries, speakers etc.). Moreover, "homeland" audience is much more connected to various precise aspects of both domestic and external affairs, pushing therefore towards a bigger transparency and accountability of its representatives, irrespective of diplomatic or security assignments formally invested. This also involves an ethical dimension in order to avoid that the interaction of the two domains lead to a form of manipulating intrusions in any way – both being equally possible (Pinkus, 2014).

Public diplomacy allows a more normal evolution in an environment marked by the omnipresence of media, yet, at the same time, it also claims the exercise of interaction skills, the achievement of new professional skills, the learning of new communication techniques and the ability to give a quick answer to a working environment continuously changing.

A comparison between intelligence and public diplomacy

In this context, the natural question about the role of secret services within the field of public diplomacy takes shape. To answer such a dilemma, a comparison between intelligence and public diplomacy, first as study disciplines and then as aspects of power, can be of great help.

The missing dimension. *The missing dimension* (Andrew & Dilks, 1984, a publication already considered part of the history of intelligence studies) presents a series of reasons about why historians were not able to observe the way and significant measure in which the secret dimension, meaning the intelligence activity, shaped the 20th century policies. Similarly, it is my belief that there are enough arguments to consider public diplomacy and its related activities as another "missing dimension".

On the one hand, this observation seems normal: it is simply difficult to understand the level and the role played by these activities in the last century, every time the comprehensive ambition is not satisfied with considering only established, formal benchmarks of classical diplomacy. On the other hand, this debate can continue: unlike historians specialized in the Intelligence activity, who can draw a map of the process, and make the necessary connections with the strategic decisions and actions, if we want to assess the impact that public diplomacy has, we will find the approach much more difficult. Often, direct causal relations are missing, leaving room to a large margin of subjective judgement. Nevertheless, the effort should not be considered useless or irrelevant.

The mechanism metaphor. The state apparatus, namely after the Second World War, meant more people and institutions/organizations in more and more places. In the intelligence field, the focus was not on working with some high class agents, but on the "industrialization" process of collecting the information, followed by the organization and knowledge management (Herman, 1996), with the development of procedures for the so-called INTs (SIGINT IMINT, HUMINT etc.), the monitoring of branches of scientific literature, or the management of complex operations etc. Diplomacy knew has known a similar evolution, towards a mechanism of different "complexes" of foreign policy (Hook, 2014), characterised by an increasing number of international connections. In this sense, we can say that the ministers of foreign affairs will keep competing more and more with other actors, among which the armed forces, the intelligence services, the direct relationships and personal skills of senior civil servants or even anonymous players from outside “the mechanism”, but who are provided with of a smartphone and find themselves in the right place and at the right moment. All these aspects are clear indicators of the exponential increase in complexity that characterises the diplomatic environment nowadays.

Decision versus effects. Both intelligence and diplomacy offer a gradated perspective of the state. If the traditional discourse about diplomacy is focused on decisions of foreign affairs policy taken by national leaders, the study of intelligence is rooted in the fact that those decisions are based on informational products shaped by complex networks of collecting, processing and disseminating information. There are many intelligence studies approaching problems such as failure, internal vulnerabilities or action motivation. In contrast, public diplomacy is less interested in the process of decision making, being mostly concerned by the *output*, the effects, however, it also deals with complex networks that try to shape the environments in which the state evolves and acts.

The emphasis given to products/effects of foreign policy reduces the attention traditionally offered to decision as a key element of diplomacy and of the state as a unitary actor. This is one of the reasons why a greater attention should be given to actor-network theories and to the way in which they are relevant for modern diplomacy (Gstohl, 2012). From such a perspective, even the strongest traditional instruments of diplomacy seem to be structurally inadequate to answer the increasingly large set of actors, requests and challenges.

Limits of open sources. Most frequently, when the relation with groups or societies relatively closed or opaque (such as Iran or North Korea) has to be dealt with, the intelligence products are an essential element: event for the simplest act of communication, it is extremely necessary to know to who you are talking, to have common subjects of interests although perspectives can diverge. Then, when also considering the relation with open states/societies, should that be on diverging matters or competitive interests, the level of public knowledge (TV, internet) about them can be quite poor and lacking structure, which means that intelligence can become an important reference to understand and choose various approaches. As a decision maker, you cannot always have a timely and accurate information by simply watching the news on TV.

How perceptions are influenced. The more delicate issue regarding the question of how to influence the perceptions of a wider audience or of personalities through key actions that are more or less discrete, cannot be avoided. It has been extensively approached by the literature dedicated to the large public, often included in articles addressing Aristotles' persuasive rhetoric in the 4th century BC, or the persuasion dynamics in the 21st century described by Perloff (2003). By focusing, however, on the perspective given by analytical pragmatism, it would be very useful if we stopped thinking in terms of the overt-covert dichotomy, and rather accept a continuum between 100% open ("message X was transmitted by government Y means") and the full range of variations from "sensitive" to "discreete but unclassified" and up to "top secret.

It is well known that even some news, in democratic societies, come from sources that are only partially open. The sentence "a close source of Minister X" is often used to avoid saying that there was an information leakage, sometimes deliberate, sometimes not, thereafter turned into news. Standard typology of propaganda – white-gray-black – can also be applied to identify sources, and common sense and wisdom of the classics (Plato's argument related to the myth of Gyges) shows that the degree of disclosure of sources is often proportional to their veracity. However, although it is reasonable to believe that a "black" source is more likely to misinform than a "white" source, it does not necessarily mean that the data provided by the former is false.

The main idea is that just like Intelligence officers, actors of public diplomacy must to assess their action environment from a variety of perspectives, sometimes by using methods borrowed from the Intelligence field.

Conclusions

The two dimensions are not brutally separated and there can be many similar aspects, some of them even transiting from one side to the other. For example, there are cases where the path of classical diplomacy is open to discrete channels of intelligence diplomacy, while others required that certain segments of public negotiation be moved backstage to avoid the pressure of the "open stage game" that can reduce the actors' flexibility to engage in a dialogue. At this point, practitioners of authentic intelligence diplomacy converge in considering that one of the important rules linking public negotiations and discrete initiatives consists in making sure that what is said behind the scenes is similar to what is assumed in public – meaning that the assessments and secret commitments must be consistent with and backed by signals transmitted in public. Otherwise, beyond the obvious moral issue and the risk of depreciation, it can also produce confusion about the real intentions and options.

Least but not last, it is necessary to show an ethical conduct designed to prevent and counter the risk (such as that of manipulation, distortion or politicization of the intelligence activity conducted for purposes of public diplomacy). The lack of ethical dimensions can damage the consistency and coherency of the decision making process, and, in addition, might lead to the reduction or even the loss of public confidence – a central element both for the intelligence activity and public diplomacy. Furthermore, a close reflection is needed, consisting of how intelligence diplomacy will evolve in the future, the changes that are still needed in both areas, as well as the strategies by which one can serve the purposes of the other without breaching ethical boundaries and damage the trust they are given by both the state and especially the citizen.

In this moment, comparative studies are still insufficiently treasured. However, given that research of public diplomacy is still developing, such questioning at the intersection of knowledge and action can be useful, providing the driving force of further developments.

References:

1. Andrew, C., Dilks, D., (1984), *The Missing Dimension: Governments and the Intelligence Communities in the 20th Century*, Basingstoke: Palgrave Macmillan.
2. Aristotel, (2004), *Retorica*, Univers Enciclopedic.
3. Barston, R.P., (2014), *Modern Diplomacy*, Routledge.
4. CIR – the US Committee on International Relations, *The role of public diplomacy in support of the anti-terrorism campaign,* October 10, 2001, retrieved from http://commdocs.house.gov/committees/intlrel/hfa75634.000/hfa75634_0.HTM.
5. CPD – the US Advisory Commission on Public Diplomacy, *Assesing US public diplomacy – a notional model*, 2010, retrived from http://www.state.gov/documents/organization/149966.pdf.
6. Dima, Dan, (2013), *Noua practica diplomatică – Diplomația publică*, Euroinfo.

7. Eriksson, Johan, Giacomello, Giampiero, (2006), *The Information Revolution, Security, and International Relations: (IR) Relevant Theory?*, in *International Political Science Review,* vol. 27, no. 3.
8. Gilboa, Eytan, Muntean, Mihai, *Diplomaţia publică şi diaspora*, contribution to European Forum for Public Diplomacy, Iaşi, Romania, 8-10 September 2014.
9. Gstohl, Sieglinde, (2012), *Diplomacy in the 21st century is network diplomacy*, The Free Library, 01.04.2012, retrieved from http://www.thefreelibrary.com/Diplomacy in the 21st century is network diplomacy.-a0316796858.
10. Hayden, Craig, (2013), *Envisioning a Multidisciplinary Research Agenda for Public Diplomacy*, E-IR open access, retrieved from http://www.e-ir.info/2013/01/11/envisioning-a-multidisciplinary-research-agenda-for-public-diplomacy/.
11. Herman, Michael, (1996), *Evolution and outline*, in *Intelligence in Peace and War*, Chapter I, Royal Institute of International Affairs.
12. Hook, Steven, (2014), *The Foreign Policy Bureaucracy, in U.S. Foreign Policy: The Paradox of World Power*, Chapter VI, Sage CQ Press.
13. Jones, Jeffrey B., (2005), *Strategic Communication: A Mandate for the United States*, in Joint Force Quarterly, no. 39, pp. 108-113, retrieved from http://www.dtic.mil/doctrine/jel/jfq_pubs/1839.pdf.
14. Kissinger, Henry, (1998), *Diplomaţia,* Ed. ALL.
15. Melissen, Jan, (October 2011), *Beyond the New Public Diplomacy*, Netherlands Institute of International Relations 'Clingendael' Paper No. 3, retrieved from http://www.clingendael.nl/sites/default/ files/20111014_cdsp_paper_jmelissen.pdf.
16. Miculescu, Simona, (2005), *Relaţia dintre presă şi diplomaţie – război sau pace?*, retrived from http://www.praward.ro/resurse-pr/articole/relatia-dintre-presa-si-diplomatie-razboi-sau-pace.html.
17. Perl, Raphael, (2006), *Combating Extremist Ideologies: Measuring Effectiveness – Considerations for Public Diplomacy*, in Connections QJ, vol. V, no. 4, pp. 64-72, retrived from http://www.pfpconsortium.org/ file/combating-extremist-ideologies-measuring-effectiveness-considerations-for-public-diplomacy.
18. Perloff, Richard, (2003), *The dynamics of persuasion: Communication and attitudes in the 21st century*, LEA, retrieved from http://staff.uny.ac.id/sites/default/files/pendidikan/dwi-budiyanto-spd-mhum/e-book-dinamic-persuasive.pdf.

19. Pinkus, Jonathan, (2014) *Intelligence and Public Diplomacy: The Changing Tide*, in Journal of Strategic Security 7, no. 1.

20. Thatcher, Margaret, (May 5, 1985), *Speech to American Bar Association*.

INTELLIGENCE IN THE 21ST CENTURY

NEW CHALLENGES ON THE INTELLIGENCE FRONTLINE – A PRACTITIONER'S PERSPECTIVE

Florian COLDEA[*]

Abstract

This century has come with different types of challenges in security matters that set a new security agenda for multiple fields, including intelligence. We all live in a growingly complex IT ecosystem, where the availability of the technology is pushed to lower levels, the security of information is fragile, and the citizens change the ways they communicate with one another and with states and governments. The technology-related change is affecting the intelligence agencies ability to deal with some of the most important threats, ranging or coming from the cyber arena, hybrid warfare, large scale migration flows, terrorism, counterespionage and other. Tackling these phenomena is not an easy task for the intelligence field requiring a comprehensive and reinforced cooperative approach, mutual support and assistance, doubled by the responsibility at state levels in decision making.

Keywords: challenges, gaps, security agenda, technology, innovation, way forward.

Introduction

The Problem. The XXI century comes in front of us with some different types of challenges in security matters. From the already "old" Y2K computer rollover problem in 2000, to the major and continuous terrorist plots in many western cities, to a series of disasters related to natural phenomena or large scale migration, to the tremendous security issues raised by the "Internet of things", people, states and societies are confronted with a new security agenda, in many ways different to what we experienced in the 20th century, with its nearly "frozen" set of threats.

Some specific situations. That new security agenda and its challenges have some specific information related aspects. In most of the cases, the threat is directly related to information (Jouini, Rabai & Aissa, 2014), as in all that

[*] Romanian Intelligence Service.

series of cyber attacks against state or private owned information systems. In others, the leaders or crisis managers need critical information that they cannot obtain because of the lack of a solid institutional or organizational infrastructure (Suchan, 2002).

Other challenges require a smart mix of secret information (from human or technical sources) and complex data already available, but not really integrated in a viable intelligence system (Delaforce, 2013).

People & administrations meet technology

The advance in communication technology in the early part of the twenty-first century have fundamentally altered **the way that ordinary citizens communicate with one another and with their states & governments**. This has demonstrably changed the character of social relations in modern societies, patterns of commerce, and relationship between the citizen and the state (Goldsmith & Crawford, 2014). The ubiquity and availability of technology is changing the face of security and privacy, and intelligence professionals must understand the current trends if they want to meet the new challenges.

As **technical collection and storage has become more accessible** to a greater range of government departments, so the number of mass population databases and the like have emerged that lay bare a wealth of sensitive information to different state agencies and those they engage with in the name of security or, more often, in the name of service delivery.

These agencies are not limited to intelligence and policing agencies – as most people still believe –, but also extend to include local administration and tax collection authorities, for example. This is a large extension of the powers granted to agencies not engaged in security and policing work.

The use to which data is put by different domestic authorities has caused considerable concern to most of privacy campaigners (being as they include information on biometrics, images, money transaction records, medical records etc., among many classes of information).

But is **the leakage & collection of this type of data by the private sector** (and the use it might be put to), and the number of access points where data could be illegally accessed by adversaries, that **is a separate and larger cause of concern**.

To sum up, if the availability and usability of the technology is pushed to lower levels, on the contrary, the knowledge needed in order to secure information is not being pushed down, not at the same speed, at least. In this manner, the security of information is more and more fragile, in direct proportion to the use that is made by states and, even so, by the private sector.

The presence of that entire technological infrastructure creates what we could call an "ecosystem", in essence, a 24/7 operating system in which servers, networks and apps are sending and receiving data to/from some other servers, networks and apps – all hopefully in the interest of states, companies, and the people or clients they serve.

States loses monopoly over technology: the gap challenge

The last decade we witnessed a shift in the technological paradigm, generated by an exponential increase in the budgets that private actors dedicate to new technologies, both for development and integration in the "business as usual" process – leaving behind the former "stars", the state actors. It has become clear that states are no longer the main drivers in the technology development, and institutions must adapt in order to keep the rhythm now is imposed by private actors and to respond to the changing expectations of the society. **This gap** between technological advancement and state capability represents **a new and strategic vulnerability** – as it challenges the institutional ability to use the latest advancement in technology, even in major crisis situations.

Andrew Parker, Director General of the MI5, points out that „**the chronic yet critical challenge we face comes from technological change**" (adresa from January 8, 2015), because the technology-related change is affecting our ability to deal with some of the most important threats.

This is not a surprise: the ability to access terrorist communications is vital to intelligence agencies ability to keep their countries safe. The internet has changed so many aspects of our lives – better in so many ways, revolutionizing commerce and communication, providing multiple choices and better access to information for us all. But also, as the examples showed early enough, it offered the same advantages and opportunities to terrorists too (Weimann, 2004).

All the greatly praised virtues of the Internet – easy access, no or little regulation, large and global potential audiences, fast flow of information, and much more – have been turned to work in the advantage of groups determined to terrorize societies in order to achieve their goals. In these days, all active terrorist groups already have an established presence on the Internet, sometimes in a very dynamic way: websites, groups and networks suddenly emerge, frequently modify their formats, and then swiftly disappear – or, in many cases, seem to disappear by changing their address but retaining similar content or membership.

They use it to spread propaganda, to radicalize impressionable individuals, to arrange travel, to move money; but most of all to communicate with one another, to plan and organize. They use the same communications tools as the rest of us. But technological and market changes risk closing off areas where we need to be able to operate.

The dark places from where those who wish to harm us can plot & plan are increasing. So, we – the state, societies, and agencies – need to keep the rhythm and not allow this technological gap to become a new territory and source of not-manageable threats.

Threats and technological change

The cyber "arena". Nowadays a broken or failing USB stick could induce more damage than a classical bomb or missile. The cyber threat not only changes the face of warfare, but also poses great risks to states and citizens. Cyber warfare is a relatively new phenomenon, its emergence being justified by our growing dependence on the cybernetic infrastructure and facilities, but also by the very low cost of transforming this tool intended for work and communication to an immaterial weapon that has a highly offensive potential. There are multiple changes in the conventional paradigm of the battlefield, and this cyber approach seems to operate a shift from means to end (Sharma, 2009) – a very good reason to understand and keep up with the permanent evolutions that take place every day in IT.

From a professional perspective, these IT evolutions must be viewed in relation to what already represents a challenge for the security field, and within this perspective it is clear that they become a new trigger for both older and recently discovered threats (espionage, sabotage, disinformation, energy, etc). It is also commonly accepted that we witnesses the creation of a new so called "confrontational arena" (Kostopoulos, 2008, pp. 165-169) – the cyberspace – with its own new kind of vulnerabilities, risks and opportunities.

Cyber attacks happens every minute in the world and even if only a very small part of them have **the potential to harm national security**, the consequences already proved to have the potential to be disastrous.

For all intelligence agencies it is vital to keep pace in this new arena, to remain competitive in their ability to tackle the challenges coming from it. The SRI expanded his cooperation with his partners (both at national and international levels) and created a Cyberint Center[1] to help protect and ensure the needed resilience of this vital core of critical infrastructure of the state and society, the IT systems.

As the doctrine in this field tend to change with every major attack or "leapfrog" in technology, intelligence agencies need to operate under a flexible and upgradable set of norms that empowers them to efficiently respond to

[1] More details on the set up of this specialized structure available on the official website, http://www.sri.ro/cyberintelligence-en.html.

new cyber threats, but within a clear legal framework that doesn't expose neither the citizens, nor the state and the institutions.

Counterintelligence in the information era. The rapid pace of technology has brought new problems and opportunities for the agencies and agents involved in counterintelligence activities. There is an incredible amount of information already available on internet, and relatively accessible to other agencies or even "ambitious" individuals, giving the possibility to access or aggregate secret information. Ten years ago, a newspaper was able to create a list of thousands of CIA agents, dozens of internal phone numbers and even more classified facilities, home addresses and cover names simply by thoroughly scanning commercial databases that were available online (Crewdson, 2006).

If, usually, technology is supposed to facilitate the rapid and large distribution of information, the role of the counterintelligence is to block the access to one's agency or state information. It is very important that CI rapidly adapt to the new operational conditions implied by the information age.

But this responsibility is not to be placed only on the shoulders of intelligence officers/agencies: partly because some of them are not technically prepared to ensure high levels of security against worldwide skilled hackers or armies of hackers, partly because most agents and information are vulnerable by reasons beyond their responsibility, such as indexation in multiple administrative databases, facial recognition facilities, poor security design of critical IT infrastructure etc.

Challenges must be approached at a wider level, by state or even allied policies, articulated into a vision that involves integrated approaches regarding people, processes and infrastructures, a vision that takes into account classical human threats and the ever rapidly growing technical threats. A new mix of resource management and training programs is needed in order to out pass the current organizational and cultural obstacles that still separate counterintelligence from intelligence and other types of activities relevant to the outcomes. Modern (and often expensive) technologies are required to enhance CI wide spectrum of operations. And last but not least, there is a vital need in the overall process, namely to obtain and maintain the trust of citizens, that our counterintelligence policies are structured and implemented in a strictly legal framework, free of suspicion and fear.

Hybrid warfare may be a *new challenge*, but its main elements are not really new (Wilkie, 2009). We all have seen before energy security used as a political weapon, or conventional military maneuvers combined with powerful cyber attacks and increased propaganda spread through new media. I think this "not really new" idea should be further debated among military thinkers, as we see that the conflicts of our times are getting more and more complex.

Although there is no unanimously accepted definition, we can easily understand **hybrid warfare as a "cocktail" or a "mix"** of classic military forces, insurgencies, terrorism, organized crime, and advanced technologies. This type of warfare can include violations of international laws, often by „private" actors, backed by states with questionable agendas. All this may be mixed together in different settings and proportions and, even more, any ingredient may be in or out at different phases of the hybrid warfare.

So is there anything new with the hybrid war? It may well be the fact that recently we have witnessed a use of its main components on a larger scale and in a more coherent manner. That's what is new: the *scale* and the *focus*. And the Ukrainian conflict almost represents a "case study" opportunity for any security practitioner interested in this type of warfare.

As Clausewitz (1989, p. 593) found: "every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions". And, as such, even if the concept of hybrid war is not really new, the intelligence and security professionals must take into account that its means are growing increasingly sophisticated and deadly, and require a proper response.

This may mean that in our constant effort to update the principles and theories of war, ultimately we have to see what parts of them still remain constant. In this field there is no "cycle" that conducts to new revolutionary panacea every decade, but permanent and incremental changes are part of business as usual in security matters. True "revolutionary paradigm changes" are less prone to occur than most conference speaker seem to believe.

At the NATO level, as I already explained in another paper (Coldea, 2016) – under the evidence of cyber attacks that hit Estonia in 2007 – the subject was discussed for the first time in January 2008, and further debated at the NATO Summit held in Bucharest in April 2008.

Terrorism proved to be a multilayered and very dynamic phenomenon, remaining one of the main threats to national and international security – mainly because it constantly traversing a changing curve. What we believe to know about this phenomenon at a certain moment may not be well suited to counter it in the future, because if the root causes remain relatively constant, the modus operandi and the tactics, the structure and organization constantly evolves. It is what makes terrorism a permanent challenge for intelligence agencies and such a vast topic of research for academia.

The constant evolution of terrorism pushed this phenomenon under the conceptual umbrella of hybrid threat, as it clearly is the case with the

Daesh and its "state like" ambitions – raising new challenges for all state institutions and security practitioners. Another example is the growing flow of foreign fighters and returnees to/from conflict areas, mainly Iraq and Syria (*Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, decembrie 2014) – a flow not only of persons, but also of military skills and radical ideas, logistical and financial support, terrorism promoters and even perpetrators.

To put things in perspective, to some extent similar to the hybrid issue, it must be said that the foreign fighters problem is not a new phenomenon. In XX century dozens of insurgencies have gone international and there have been foreign fighters in many modern civil wars, many voices counting English poet Lord Byron as a foreign fighter in Greece in the 1820s (Malet, 2010, p. 101). What is new in present times is the scale of the threat raised with the outbreak of civil war and sectarian violence in Syria, Iraq, Libya, and other countries.

Tackling these phenomena is not easy, as it has become more and more clear in the recent years. It **requires a comprehensive and cooperative approach**, as it is an international rather than a national issue and can only be addressed effectively by common efforts of more than a few countries and/or agencies. We have seen that after each major attack (Paris 2015 and 2016, Bruxelles 2014 etc.) the respective national judicial norms are updated, mainly by framing new terrorist offences. It is a common and foreseeable reaction to the growing threat, but that may also create some new risks related to the lack of common standards or even prosecution and criminalization gaps across different but similarly exposed countries.

In that context, the need to enhance international cooperation has become more and more evident, and may be further reinforced by multi-disciplinary approach (judicial, intelligence…). None of us can deal with this threat alone, so close and applied cooperation is required.

Immigration. The number of immigrants and refugees was raising sharply in 2015 and has become quickly a prominent matter on European political and security agendas, confronting the decision makers with key issues regarding: the impact on the transit and destination countries (*Countries of transit* ..., 11 septembrie 2015), the impact on the common European ties and solidarity (Goldner Lang, 2015), the measure in which the globalization has become a catalyst for large population movements, what respective roles for state institutions and civil society etc.

From a security perspective, the main error is to think and frame this issue in limited domestic terms, as it actually is a pan-European problem caused by a pan-Arab arch of conflict and instability. Across the European countries, the policy issues and the main items of debate are very similar, in some cases overlapping sensitive matters as security, identity and ethnicity. This proves, once more, that it is a common issue requiring solidarity among member states in reciprocal support and assistance.

If we want to keep things in perspective, while the truth is that no one knows what will happen to immigration trends on the short and medium run (the long term probability being that small wars and the urbanization trend of the world's population will keep the immigration numbers high), it is the common responsibility of states that will help us to deal with the issue and to protect our national and regional security.

The perspective of "high numbers" generates new risks, also relevant for the law enforcement agencies and the security and information services. These institutions must adapt and adjust their resources (human and financial) and need to operate in an updated legal framework.

Conclusions of the way forward

The rhythm of technological change and innovation had left behind regulation, and oversight in the past decade. Without a serious update of the law and oversight regarding these technologies and practices, and without honest and open debates over the extent of surveillance by public and private sources, this gap will become even wider.

States and societies must adapt their reflexes to this world of growing interdependence and interaction even between apparently distinct issues such as terrorism and health, and between actors, such as people, government and industry.

The key challenge here is **to build state capabilities,** to set up and support solid institutions, based on democratic principles, and always keeping an eye on their professionalism, accountability and integrity.

I believe it is our responsibility, as intelligence professionals, to **keep pace with these rapid developments** in the actual volatile security environment and to propose **new imaginative solutions** in order to ensure and protect the security of the citizens.

All these challenges are to be **better understood by common efforts** (among decision-makers, practitioners, academics) so we can achieve a deeper knowledge of the matters and we can recommend viable solutions. This manner of approaching difficult subjects favors **the exploration of new perspectives** and paradigms

We must continue to search for new ways to manage all these relationships **at a time when the public demand for information and transparency is higher than ever**.

References:

1. *Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI) at Thames House*, January 8, 2015, available on https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html.
2. *Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, Global Center on Cooperative Security, Human Security Collective, and International Centre for Counter-Terrorism – The Hague, Policy Brief, December 2014.
3. Coldea, Florian, (2015), *Building national capabilities and countering hybrid threats: lessons learned*, Key Note Speech at NATO Advanced Research Workshop on *Countering Hybrid Threats: Lessons Learned from Ukraine*, Bucharest, 2015 September 28-29th.
4. *Countries of transit: meeting new migration and asylum challenges*, Council of Europe Committee on Migration, Refugees and Displaced Persons, Doc. 13867, September 11, 2015, available on http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=22017&lang=en.
5. Crewdson, John, (March 12, 2006), *Internet Blows CIA Cover*, in Chicago Tribune, available on http://articles.chicagotribune.com/2006-03-12/news/0603120396_1_agency-employees-or-operatives-cia-director-porter-goss-two-dozen-secret-cia.
6. Delaforce, Ruth, (2013), *Public and private intelligence: historical and contemporary perspectives*, în *Salus Journal*, Issue 1, Number 2, available on http://www.salusjournal.com/wp-content/uploads/sites/29/2013/03/Delaforce_Salus_Journal_Issue_1_Number_2_2013_pp_21-39.pdf.
7. Goldner Lang, Iris, (2015), *The EU Financial and Migration Crises: Two Crises – Many Facets of EU Solidarity*, in E. Dagilyte & E. Küçük (eds.), *Solidarity in EU Law: Legal Principle in the Making*, Edward Elgar Publishing.
8. Goldsmith, Stephen, Crawford, Susan, (2014), *The responsive city. Engaging communities through data-smart governance*, San Francisco, Jossey-Bass.
9. Jouini, Mouna, Rabai, Latifa Ben Arfa, Aissa, Anis Ben, (2014), *Classification of Security Threats in Information Systems*, Procedia Computer Science, Volumul 32, pp. 489–496.
10. Kostopoulos, George K., (2008), *Cyberterrorism: The Next Arena of Confrontation*, Communications of the IBIMA 6(1), pp. 165–169, available on http://www.ibimapublishing.com/journals/CIBIMA/volume6/v6n25.pdf.
11. Malet, David, (2010), *Why Foreign Fighters? Historical Perspectives and Solutions,* Published by Elsevier Limited on behalf of Foreign Policy Research Institute, Winter 2010.

12. **S**harma, Amit, (2009), *Cyber Wars: A Paradigm Shift from Means to Ends in The Virtual Battlefield: Perspectives on Cyber Warfare*, Proceedings 2009, NATO Cooperative Cyber Defence Centre of Excellence, available on https://ccdcoe.org/sites/default/ files/multimedia/pdf/01_SHARMA_Cyber_Wars.pdf.
13. Suchan, William, (2002), *The organizational information infrastructure maturity model*, AMCIS Proceedings, Paper 295, available on http://aisel.aisnet.org/cgi/viewcontent.cgi?article= 1654&context=amcis2002.
14. Von Clausewitz, Carl, (1989), *On War,* Princeton University Press.
15. Wilkie, Robert, (2009), *Hybrid Warfare: Something Old, Not Something New*, în Air & Space Power Journal - Winter 2009, available on http://www.airpower.maxwell.af.mil/airchronicles/ apj/apj09/win09/wilkie.html.
16. Weimann, Gabriel, (March 2004)*, How Modern Terrorism Uses the Internet*, US Institute of Peace, Special Report 116, available on http://www.usip.org/sites/default/files/sr116.pdf**.**

FRENCH ECONOMIC INTELLIGENCE SYSTEM

Loredana IVAN[*]

Abstract

„Economic intelligence" or „State level competitive intelligence", a relatively new subject regarding international intelligence concerns, aims to augment economic competitiveness and to create synergy between state and private interest, for maximum efficiency and effectiveness in the competition for resources and markets. Information, as a production neo-factor, when it is properly processed and valued, has the potential to significantly contribute to the growth and consolidation of the national economy. France is one of the pioneers of the international scene, that managed to obtain great results in the design and implementation of a national economic intelligence.

Key words: Economic intelligence, France, national interest, risks.

Introduction

The competitive environment is what makes the market function efficiently, but competitive performance in economy depends on monitoring economic relations and adjusting them using public policy. Governments are forced to permanently adapt the economies, which generates a permanent need for actual and accurate information. To prevent and counteract the unwilling effects of competition on a global market, economic advanced states use competitive improvement systems for their economies, gathering, processing and analyzing data and information being an important tool.

Some countries – Japan, France, USA, Great Britain etc. – have chosen, in the postwar era – to develop and implement genuine force strategies, destined to make them capable to handle challenges associated with economic competition on a global scale, and, in this spectrum, the French typology has quickly and obviously detached, especially by placing economic intelligence on a state policy level.

Shortly after World War II, Japan has projected a complex system of gathering and processing economic information, with the main contribution from the Industry and Exterior Commerce Ministry, thus, making possible to recuperate the offset in several areas such as: naval and automobile construction, construction machinery, IT, robotics etc.

[*] PhD Student, "Mihai Viteazul" National Intelligence Academy.

Since 1994 – with the report *Intelligence économique et stratégie des enterprises* (Martre, Clerc și Harbulot, 1994), France has given a major importance to information from the economic area, building a national system for gathering, processing and using information, useful to economic operators to implement their own business strategies.

Since 1995, the USA Security Strategy has been based on three pillars: the military, the economic and the cultural one, the Washington Government investing enormously in developing its own capabilities to "feed" the administration and the entrepreneurs with economic information (USA Security Strategy, 1995).

Since 1998, Great Britain has placed the issue of information in the center of its economic strategy – defined in the report *Our competitive future: building the knowledge driven economy* (1998), with the scope of adjusting administrative policies to help British companies.

Germany also managed, in the '90s, to correlate the objectives of the state/lands with those of the (big, medium and small size) economic operators, through systematic dialogue on subjects such as competitive information, finally building a strong system connected to the ordo-liberal economic doctrine (22 Review, no. 304).

Other countries are in the situation of not being able to harmonize the objectives of the companies with the official ones, on a state policy level, so there are not yet defined national economic intelligence strategies, but important economic actors from these states – such as Spain, Italy and Portugal – have complex programs of competitive intelligence.

Neither does China have a formalized national economic intelligence strategy, in the Western style, but Beijing understands that the global competition is mostly economic, thus, since the late '90s, the Chinese Government has conducted its policy based on information, especially focused on controlling the technology of the future. The results are visible for anyone and anywhere.

On the other hand, the former communist countries do not have national programs or significant initiatives to catch up with developed countries. The internal political competition in these countries made impossible the emergence of genuine concern in this area. Even more, because of the inexistence of a solid administrative capacity and the tendencies for corruption of some segments of the state apparatus, in the last decades, major errors have occurred in domestic economy, which augmented the delays as compared to the countries that have understood what arsenal is needed, at present, in order to conquer people's minds and territories.

Concepts

Economic intelligence or competitive intelligence on a state level is a relatively new issue among international intelligence works, with a special focus in France. The concept has developed through a dual process of practice standardization and the emergence of a scientific community, becoming a distinct matter of study in the last 20 years.

Henri Martre, the coordinator of the Report of the Plan Commissariat, named *L'intelligence économique et la compétitivité des enterprises* (1998), defines economic intelligence as the totality of coordinate actions of gathering, processing and distributing information useful to the economic operators for implementing business strategies (1994, pp. 16-17). These different actions take place legally, with all the necessary protection guaranties for protecting the wealth of the company, with the best conditions in terms of quality, time and costs. Useful information is necessary to different decision makers of the society or community, to develop and implement, in a consequent way, the strategy and tactics necessary to enhance their position in a competitive environment. These actions, in a company, are organized in a perpetual cycle, generating a common vision on the company objectives.

According to Christian Harbulot (*Intelligence economique*), economic intelligence is defined as systematic researching and processing of available information, to decipher the intentions of the competitors and to learn their capabilities. It includes all operations of surveillance of the competitive environment (protection, monitoring and influence) and it differs from traditional intelligence (*Intelligence economique*) by:

- the nature of its area of applicability (because it refers to open information, thus necessitating conformation to credible ethics);
- the identity of its actors (considering that the staff and the personnel structure - and not exclusively experts - can participate in the construction of a collective information culture);
- cultural specificity (because each national economy produces an original model of economic intelligence, whose impact on commercial and industrial strategies varies from country to country).

In the Report *Intelligence économique, compétitivité et cohésion sociale* (Carayon, 2003), presented to the French prime minister in 2003, deputy Bernard Carayon made economic intelligence a public policy of competition, economic security, influence, especially among international organizations, and training. Economic intelligence derives from a particular understanding of globalization, which takes into consideration daily characteristics of markets, avoiding the law and power and influence games. It is a new approach which the author considers essential, just as there were, in their times, the city policies, the policies for sustainable development etc. Economic intelligence is a public policy by content and applicability. Its content is represented by the economic security of the state. Thus, economic intelligence must define the activities that need to be protected and the means to achieve this goal. In addition, it defines the ways to support companies on global markets, and, also, the ways to influence international organizations which settle regulations and standards applicable to states, enterprises and citizens (Carayon, 2003).

In turn, Claude Revel (*Intelligence economique*) emphasizes that economic intelligence has the purpose of knowing external environment in order to properly adjust the behaviour. It identifies opportunities and determinant factors of succes, it anticipates the threats and prevents the risks, in order to secure, act and influence the environment from the perspective of international competition.

Claude Revel talks about three functions of economic intelligence (*Intelligence economique*):

- information management (gathering, selection, validation and processing necessary and pertinent data about competitions, characteristics and regulations of the markets);
- protecting (ensuring physical or any other type of security, which means the ability to anticipate risks on intellectual property, image or capital of a firm/firms);
- influencing competition (represents the ability to argue, convince, negotiate, professional lobby, exercise a normative influence by anticipating international regulations and standards and, possibly, involving in their development).

Economic intelligence allows a better learning about competition, principles, regulations and standards which can influence the activity and, thus, ensure an adequate action capacity on specialized markets. Economic intelligence is based on ethic mechanisms and it totally differs from espionage, theft and influence peddling.

Also in France, Christophe Deschampes and Nicholas Moinet (2011) argue that in the context of globalization and growing world competition, economic intelligence – as a way to obtain strategic information, useful to economic agents – constitutes, more and more obvious, a stringent necessity. Economic actors, regions and states cannot ignore and must impose and use this essential function for market consolidation, guarantee of quality and, recently, sustainable development.

In Romania, Valeriu Ivan (2014) emphasizes that economic intelligence or competitive intelligence on state level, a relatively new matter among international intelligence issues, tries to augment economic competition and to create synergy between private interests and those of the states, for maximum efficiency and efficacy in global competition for resources and markets. Information, as a production neofactor, correctly processed and used, has the potential to significantly contribute to the growing and consolidation of national economy.

Coordinates of the French Economic Intelligence System

Key Historical Moments. After the works of some pioneers (Jacques Villain, Philippe Baumard, Amiral Pierre Lacoste, Henri Dou, François Jakobiak, Vahe Zartarian[1]) economic intelligence was officially introduced in France, in April 1992, by creating the French branch of Society of Competitive Intelligence Professionals (SCIP – France), at the initiative of Robert Guillaumot, Yves-Michel Marti, Bruno Martinet and Jean Pierre Bernat[2].

In 1994, the Report of the General Plan Commissariat *Intelligence économique et stratégie des enterprises*, also named Martre Report (after the name of its author, Henri Martre, former chief of the Aerospatiale structure), confers legitimacy to the state in this new area. The idea of creating a study group on this matter is included in the Plan by Philippe Baumard and Christian Harbulot. The group was informally constituted and it included, in the majority, people closed to Philippe Baumard and Christian Harbulot, which was a premiere in this field.

In April 1995, the Committee for Economic Competition and Security was created, near the French prime minister, with seven members elected for two years (company managers, scientists and syndicates). This for has become old-fashioned since 1997, during the Government of Lionel Jospin, who did not name new members in the Committee. The main mission of this forum was to inform the prime minister with issues of competition and economic security, counseling with projecting and implementing the public policies.

A Report sent to the President of France, published with the Decree no.95-350 from 1st of April 1995 emphasizes the role of information as a strategic resource and the determination of the state to concentrate all its energies on the main national challenge that is economic intelligence[3]. This was set into practice by establishing clear priorities. The first of these priorities refers to orientation towards the necessities of enterprises, especially small and middle ones, to gain access to information and the requirements for redirecting public data gathering and processing facilities.

[1] Published in `80, see details on http://www.portail-ie.fr/article/571/Historique-de-l-intelligence-economique (accessed on 01.06.2015).

[2] SCIP reunites 400 members in France a 6000 in 50 countries.

[3] See details at https://www.bo.sga.defense.gouv.fr/boreale_internet/popup.php?no_cache=2&mode= 1&txt_id=194446&format=pdf& (accessed on 01.06.2015).

The second priority refers to promoting interaction between public authorities and private ones, on matters of economic intelligence, for creating and coordinating information exchange networks. The third priority refers to developing a set of practices, by disseminating on a large scale an economic intelligence approach, through university and business schools courses. In addition, it is noticeable a regional dynamics, of training and awareness programs for the small and middle enterprises. The first experimental initiative on a national scale was launched in the Parisian region in October 1995, for a year, on a sample of 300 companies.

In 2000, two American investment funds, suspected of connections with the CIA, Texas Pacific Group and Spectrum Equity Investors tried to take control over French company Gemplus, world leader in electronic cards (*Intelligence economique*). The French Exterior Minister was warned twice about the EUTELSAT[4] file, which was then targeted by the same two investment funds.

In June 2003, deputy Bernard Carayon presented to the French prime-minister the Report *"Intelligence économique, compétitivité et cohésion sociale"* which approaches economic intelligence as a public policy destined to ensure social cohesion through economic development. In one of the Reports annexes there are several definitions, some contradictory, precisely to demonstrate the difficulties of defining economic intelligence.

Among the effects driven by the Report of Nernard Carayon is the appointment (in 2003) of a high representative in the field of economic intelligence (Haut Responsable a l'Intelligence Économique – HRIE), near the prime minister, but also the establishment of competitive poles, during the mandate of Dominique de Villepin, and, respectively, the implementing of a new territorial intelligence policy, during Nicolas Sarkozy's mandate (*Intelligence economique*).

Institutional Mechanisms. ***On the 31st of December 2003, Alain Juillet was appointed high representative for economic intelligence of the General Secretariat of National Defense (Secrétariat général de la défense nationale – SGDN), because of his particular credibility on a national level, given by the key positions he had in the fields of business and French intelligence services, which came over his lack of experience in the field of competitive intelligence. A General Delegation for Economic Intelligence was created in Bercy and, on the 12th of October 2004, François Asselineau was appointed general manager of this forum*** **(Intelligence economique).**

[4] EUTELSAT is a French-based satellite provider. Providing coverage over the entire European continent, as well as the Middle East, Africa, India and significant parts of Asia and the Americas.

In September 2005, "sensitive" sectors were defined, with the public announcement made by the ministry of industry; regarding the adjustments of the Monetary and Financial Code (mass media mentioned the fields of gambling/casinos, special industry, cryptology, biotechnology, information systems security etc.). Also in September 2005, it was ensured the coordination of the activities of the sustainable development interministerial representative and the high representative for economic intelligence.

In August 2006, the ministerial coordinator for economic intelligence was appointed within the ministries/departments of Bercy (*Intelligence economique*). An economic intelligence system was settled, within the economic and finance ministries in Paris and on regional level. Through the Circular Letter of the 21st of March (published in the French Official Gazette no. 108 from the 10th of May 2007), regional representatives for economic intelligence were created.

In the first semester of 2009, several important public activities took place, as follows (*Intelligence economique*):

- The designation of the representatives for public intelligence for different ministries (at the Exterior Ministry, a structure for each ambassador was designated and, at the Interior Ministry, Economy, Finance and Industry, there was a one representative, without a staff and without working tools);

- The implementation, by prefects, of the regional economic intelligence network;

- The establishment of a professional system for training/studying in the field of economic intelligence;

- The creation of a professional federation in the field of economic intelligence.

On the 17th of September 2009, the interministerial delegate for economic intelligence was appointed.

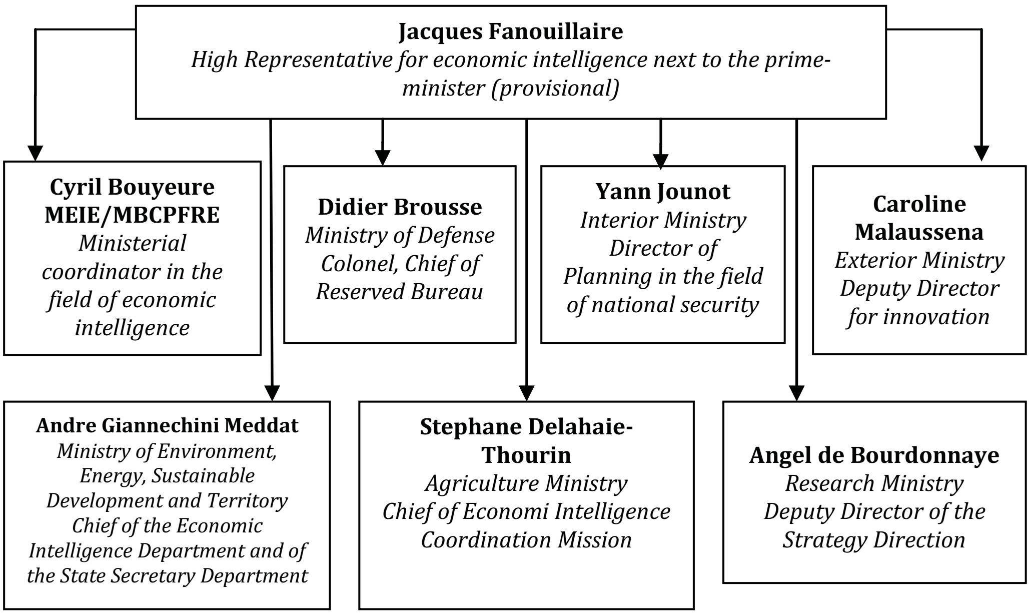
In August 2010, a new coordinator for economic intelligence of the economic and finance ministry was designated.

In the Circular Letter from the 15th of September 2011, the prime-minister declared public the state's Action in the field of economic intelligence for central authorities and deconcentrated services (*Politique-publique-d-intelligence-economique*).

On the 29th of May 2013, Claude Revel was appointed interministerial delegate for economic intelligence, a job created around the French prime-minister (*Intelligence economique*).

In conclusion, the French economic intelligence system is based on central mechanisms of implementation and also on a territorial network of regional centers responsible with this type of strategies (CRIE), which depends on the Service of Economic Intelligence Coordination (SCIE) of the ministries of economy, industry and work. The system was reformed in the last years for an increase of the performance (*Intelligence économique: historique*). Practically, the mechanism of the high representative for economic intelligence (HRIE) was replaced with the interministerial delegate and the 22 regional centers (CRIE) came under the jurisdiction of the regional directorates for business, competition, consumption, work and workplaces (DIRECCTE), which, in 2010, fusioned into 7 deconcentrated administrative structures (*Intelligence économique: historique*).

The French economic intelligence system includes a central mechanism - represented in Figure no. 1 -, coordinated by the high representative and formed by the exponents of the seven major institutional structures.


Jacques Fanouillaire
High Representative for economic intelligence next to the prime-minister (provisional)
Cyril Bouyeure
MEIE/MBCPFRE
Ministerial coordinator in the field of economic intelligence
Didier Brousse
Ministry of Defense
Colonel, Chief of Reserved Bureau
Yann Jounot
Interior Ministry
Director of Planning in the field of national security
Caroline Malaussena
Exterior Ministry
Deputy Director for innovation
Andre Giannechini Meddat
Ministry of Environment, Energy, Sustainable Development and Territory
Chief of the Economic Intelligence Department and of the State Secretary Department
Stephane Delahaie-Thourin
Agriculture Ministry
Chief of Economi Intelligence Coordination Mission
Angel de Bourdonnaye
Research Ministry
Deputy Director of the Strategy Direction

*MEIE/MBPCFRE – Ministry of Economy, Industry and Workplaces/
Ministry of Budget, Public Accounts and State Reform

Figure no.1 – Economic intelligence central system – addaptation after *Intelligence économique: historique* in *Intelligence économique*: *deux nouvelles missions pour l'expert-comptable*, 64th Congrès de l'Ordre des Expert-Comptables

On territorial level, the economic intelligence system from France is based on four central institutional structures (the Defense Ministry, the Interior Ministry, the Finance and Interior Ministry and the Exterior Ministry) and also on the French bicameral system, universities, the Technological Information Diffusion Agency, the International Investment Agency, the public support network, the Research National Agency, territorial associative entities etc. In large, the territorial system is coordinated by each prefect and has two types of interventions (offensive and defensive) - depicted in Figure no. 2.

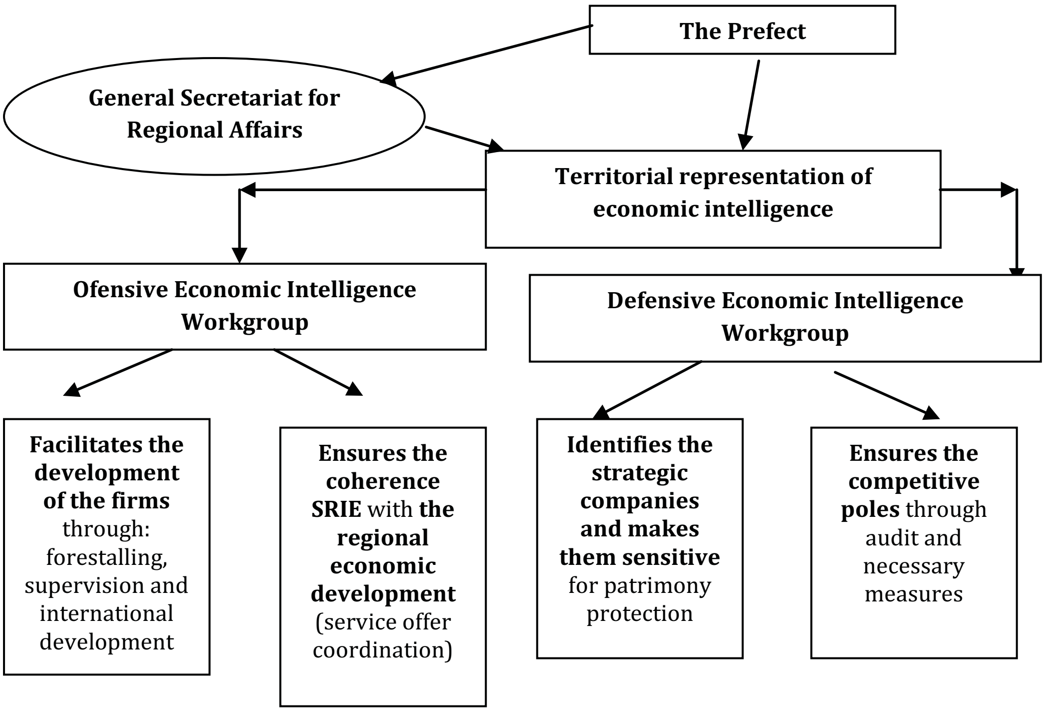

The Prefect
General Secretariat for Regional Affairs
Territorial representation of economic intelligence
Ofensive Economic Intelligence Workgroup
Defensive Economic Intelligence Workgroup
Facilitates the development of the firms through: forestalling, supervision and international development
Ensures the coherence SRIE with the regional economic development (service offer coordination)
Identifies the strategic companies and makes them sensitive for patrimony protection
Ensures the competitive poles through audit and necessary measures

Figure no. 2 – Territorial economic intelligence system (august 2009) – addaptation after *Intelligence économique: historique* in *Intelligence économique*: *deux nouvelles missions pour l'expert-comptable*, 64th Congrès de l'Ordre des Expert-Comptables

The training and improvement system in the field of economic intelligence

This is formed by the following structures, according to SMGB[5]:

- The Economic War School, from Paris, ranked 1st in France, from 2002, from 2002 to 2013;

- The European Economic Intelligence School; (EEIE) from Versailles, ranked 3rd in 2013, prepares specialists in the field of economic intelligence consultancy;

[5] SMBG is the first orientation cabinet, specialized in the training of candidates for high schools and universities.

- Poitiers Business Administration Institute (Information - Communication Pole), which organizes master courses in economic intelligence and strategic communication;

- University of East Paris Marne-la-Valle, which offers master courses of 2nd level in the field of economic intelligence and risk analysis. It was the first university school of economic intelligence, created in France in 1993 by Admiral Pierre Lacoste;

- École d'Ingénieurs Génie Informatique Génie Mathématique (EISTI) (ranked 4th in 2013, 2nd in 2014 and 3rd in 2015), which ensures master programs of 2nd level in the field of strategic analysis and economic intelligence;

- Bordeaux University offers professional master courses of 2nd level in intelligence and innovation economy (Montesquieu Bordeaux IV University);

- Paul Cézanne Aix-Marseille III University, which offers master programs of 2nd level in the field of technological intelligence and innovation;

- International Institute for Development and Commerce (ICD), which offers, in partnership with IEP Aix-en-Provence, economic intelligence certificates;

- Angers University, which ensures master programs in the field of economic intelligence and competitive strategies;

- SKEMA Business School, ranked 2nd in 2013 and offers courses of economic intelligence.

Conclusions

In France, economic intelligence has several definitions and a multitude of practices, being depicted as gathering, processing, prospective analysis and utilization of information and knowledge for enhancing the efficiency of economic actors (Baulant, 2004).

Its main objective is to grow the competitive abilities of the firms, regions and nations, through strategic information management. The tools used, adapted to present economic transformation, globalization, respectively, knowledge economy, are: surveillance, influence and network analysis.

France seems to be the first country which decided to consider economic intelligence as a national priority, following the publication of the studies realized by a group of experts, gathered within the General Plan Commissariat in 1992-1994, on the issue of *Economic Intelligence and Corporative Strategy* (Commissariat Général du Plan, 1994). The work group - formed by business representatives of the government, syndicates, universities and information professionals - has identified the strengths and the weaknesses of the French system, based on a detailed analysis of the best economic intelligence systems. Beneficiating of a rich tradition in this field, the French state plays a major part, establishing economical and technical information networks and technical progress support structures.

The French define economic intelligence as a series of coordinated actions of investigating, processing and disseminating useful information to be exploited by economic actors (Economic Intelligence in a Global World, 2014, p.16).

The definition takes into consideration two factors: on one hand, the research of available scientific resources for developing new scientific fields which may supply auxiliary economic advantages, and, on the other hand, the surveillance of the activity of the labs and factories from rival countries or factories, for the awareness of the breaches and competitive improvement (Economic Intelligence in a Global World, 2014, p. 16).

In turn, the publicity of the Carayon Report is a clear clue of the importance that these technics and services have for the French political forces, marking France's entry in a world of informational society, with all the consequences on national wealth, which consist, "beyond the human quality, in the sum of juridical, financial, commercial, scientific, technical, economical or industrial information" (Carayon, 2003). The Report warns that threats on the country's productive structure have grown, becoming more and more subtle, and the exacerbation of international competence transforms strategic information of the companies in a true "economic war".

The French system is projected and adapted to the new circumstances and necessities, so that, beyond state agencies, prestigious companies specialized in strategic intelligence are involved, as well as a network of commerce chambers which act in the interest of France, on internal and external level. It adds the territorial economic intelligence mechanisms (mainly, the regional councils and, in some cases, the general councils and the departmental communities), which participate progressively and more and more actively to the economic intelligence activities. The list continues with other structures involved in regional development (the National Institute for Industrial Property, The Agency for the Diffusion of Technological Information, The Workmanship Chambers, The French Agency for International Development of Enterprises), and also professional organizations and groups - the Information Security Clubs, the Federation of Economic Intelligence Professionals (FEPIE), The Movement of French Enterprises (MEDEF), the General Confederation of Small and Middle Enterprises (CGPME) etc.

References:

1. Baulant, Camille, (2004), *Les outils de l'intelligence économique face aux défis de la mondialisation*, Angers, available at http://master-iesc-angers.com/ (accessed on 08 June 2015).
2. Carayon, Bernard, (2003), *Intelligence économique, compétitivité et cohésion sociale*, available at http://www.bdc.aege.fr (accessed on 01 June 2015).

3. Deschampes, Christophe, Moinet, Nicolas, (2011) *La boîte à outils de l'Intelligence économique,* Dunod, Paris.
4. *Economic Intelligence in a Global World*, 2014.
5. *Intelligence économique: historique*, în *Intelligence économique: deux nouvelles missions pour l'expert-comptable*, 64ème Congrès de l'Ordre des Expert-Comptables.
6. Ivan, Valeriu, (2014), *Analiza informaţiilor: de la intelligence competitiv la componenta economică a securităţii naţionale*, Academia Românã (PhD Thesis), Bucureşti.
7. *Intelligence economique*, available at https://fr.wikipedia.org/wiki/ Intelligence_%C3%A9conomique (accessed on 01.06.2015).
8. Martre, Henri, coord., (1994) Rapport du Commissariat au Plan consacré à *«l'intelligence économique et la compétitivité des entreprises»,* La documentation française.
9. Martre, Henri, Clerc, Philippe, Harbulot, Christian, (1994), *Intelligence économique et stratégie des enterprises*, France, Commisariat general du plan, available at http://www.ladocumentationfrancaise.fr/rapports-publics/074000410/index.shtml (accessed on 21.03.2015).
10. Seal of de the President of the United States of America, A national security strategy of engagement and enlargement, 1995, available at http://www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf (accessed on 21.03.2015).
11. UK Government, Our competitive future - building the knowledge driven economy: The UK Governments Competitiveness White Paper, December 1998.
12. http://www.portail-ie.fr (accessed on 01.06.2015).
13. http://www.intelligence-economique.gouv.fr (accessed on 01.06.2015).
14. http://www.bdc.aege.fr (accessed on 01.06.2015).
15. http://www.watsoninstitute.org/gs/Security_Matrix/(accessed on 21.03.2015).
16. http://www.ladocumentationfrancaise.fr/rapports-publics/074000410/index.shtml (accessed on 21.03.2015).
17. http://www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf (accessed on 21.03.2015).
18. http://stats.bis.gov.uk/competitiveness5/Past%20Indicators/UKPC1999.pdf (accessed on 21.03.2015).
19. http://master-iesc-angers.com/ (accessed on 08.06.2015).
20. *Politique-publique-d-intelligence-economique* available at dttp://www. economie.gouv.fr/politique-publique-d-intelligence-economique (accessed on 01.06.2015).
21. http://www.portail-ie.fr/article/571/Historique-de-l-intelligence-economique (accessed on 01.06.2015).
22. http://www.revista22.ro/22-plus-nr-304-ce-este-ordoliberalismul-9048.html (accessed on 01.06.2015).
23. Official Monitor in France, no. 108/ 10 May 2007, available at http://www.legifrance.gouv.fr/affichJO.do?idJO=JORFCONT000000003492 (accessed on 11.12.2015).

INTELLIGENCE ANALYSIS

THEORY AND PRACTICE IN INTELLIGENCE: KNOWLEDGE DRIVERS

Cristina POSAŞTIUC[*]

Abstract

Cooperation with academia is seen by intelligence theorists and practitioners alike as a way to support change management, improve analytic capabilities and better cope with emerging challenges. Intelligence scholars often focus on 'big phenomena' such as social change, the shifting nature of threats or ethics in intelligence, while practitioners are concerned (in public statements, at least) with more mundane issues such as human resource management, workflow streamlining and establishing good rapport with beneficiaries.

Not even apparently clear-cut terms such as "strategic" bear the same meaning within the two groups: theorists seek to correlate social and organizational change, while practitioners are more interested in detecting risks and threats in their nascent stages so as to better prepare for "worst case" scenarios.

Managing the knowledge production process is, unfortunately, a topic which doesn't rank high with the intelligence community.

Keywords: change management, cooperation, theory and practice, knowledge production.

Specific perspectives

In order to ensure knowledge production and innovation in a competitive environment, the ability of an organization to learn and adapt must be enhanced by understanding the dynamics of knowledge processes (from structures and sources, to production, validation and application) (Crompton, 2002, p. 10).

The impact of technological and social evolutions that triggered substantial changes in both business and security environments, have forced intelligence agencies to reevaluate both their organizational structure and their objectives, as, according to Sandra Brizga and Patricia Geraghty, every institutional or personnel change presents particular challenges and opportunities for knowledge management, as there are significant risks of

[*] Romanian Intelligence Service.

knowledge and information being lost in the transition process (Brizga & Geraghty, 2011, p. 7).

Within the process of restructuring, intelligence services take into account both the possibility of outsourcing analytical activities, and of developing a modern way of performing those activities, as well as implementing openness policies. According to Lahneman (2003), a collection and analysis can be outsourced as noncore functions because the intelligence community does not have all the expertise it needs. It is also best to allow the civilian analysts to use their time on more pressing analytical areas.

The influence of new media, the increasing number of private think tanks and companies that can provide analytic support, cybersecurity, the type of relationships established with the political stakeholders are, nowadays, some of the main topics of debate among both intelligence practitioners and theorists.

Magnus Hoppe[1] states that "the knowledge perspective has not been the pinnacle of intelligence research. Instead, the field is dominated by research objectives aimed at delivering practical advice for the practitioner" (2013, p. 60).

From a pessimistic perspective, Joshua Rovner[2] underlined that the intelligence agencies face new challenges from this expanding number of think tanks and private sector analysis firms that "often portray themselves as quasi-intelligence organizations, and some actively recruit government analysts to bolster their credentials"(Rovner, 2013).

Social media have created an explosion in new sources of information, but the rise of private sector intelligence has propelled competition in order to attract policymakers' attention. Both issues raise important questions about whether and how traditional intelligence agencies can remain relevant to policymakers.

Thus, the role of intelligence, the importance of intelligence studies, the transition from a "1.0" to a "3.0" society, the need for applied methods to collect and use intelligence in decision support, and the academic training of intelligence services personnel, all these are of interest for intelligence professionals.

The need to reform in order to adapt to the knowledge society challenges has become a priority of most intelligence organizations and the

[1] Senior lecturer, School of Business, Society and Engineering, Mälardalen University, Västerås, Sweden.

[2] Associate Professor of Strategy and Policy at the U.S. Naval War College.

means of accomplishing this objective include, in most cases, consolidating the relationships with the academic world and reshaping those established with the political factor.

But there is a gap between the points of view expressed by each part that lies in the type of activity and the priorities of these actors: the practitioners' stress, above all others, the importance of ensuring national security, whereas the theorists focus on reshaping the theoretical grounds on which the intelligence activity should be based.

Challenges

Technological breakthroughs, regional instability and the risks of conflict in different regions of the world, cyber deterrence, potential rise of non-state actors, climate and demographic changes, terrorism, the increasing demand for food, water or energy are just few of the challenges that intelligence agencies everywhere focus on, in order to ensure national security.

The above mentioned focus on these trends should be synchronized with a proper vision for a consolidated knowledge society that combines the interests of all stakeholders. This perspective encompasses new solutions, a modern vision, a transdisciplinary approach, better human resources as well as a state-of-the-art technological infrastructure.

From a theoretical point of view, this task may seem easy to accomplish, maybe even in a short-to-medium time frame. But the need to provide decisionmakers with timely and efficient analytical products or to detect a risk or a threat in early stages may prevail over issues such as the role or the importance of a consolidated intelligence literature - one of the main topics of debate among theorists –, and not because the subject is of no interest, but precisely because of the pressure exerted in everyday activity by those challenges.

Some of the most important issues of debate among experts are: the nature of intelligence – methodologies, tradecraft; the issue of theory versus practice; intelligence politization; the volume of information faced both by the analysts and policymakers; the tension between civil liberties/human rights and intelligence services' operating practices; ethics; the relationship between national and international security; accountability versus efficiency (Johnson and Shelton, 2013).

As far as intelligence literature is concerned, experts such as Mark Lowenthal and Walter Dorn (Johnson and Shelton, 2013, p. 114) agree that there are policymakers as well as practitioners "far removed" from intelligence studies, as there is no time or no interest in reading "academic" products. Thus, they rarely give feedback on what they read.

Knowledge, the core of intelligence mission

According to Ruben Arcos (2013), "business, non-profit, and governmental organizations in general have become aware of the need to manage relationships with their stakeholders if they want to succeed in accomplishing their missions".

Like other governmental agencies, intelligence organizations must address their mission timely, competently and efficiently in order to provide good products and satisfy decisionmakers' requirements. There may be cases in which intelligence agencies do not have the ability to obtain public support for their actions, considering the covert nature of some of the operating practices. A lack of public perception or understanding of their mission and practices can decrease consumer support.

In the last years, the role of the academic world in the field of intelligence has become strategic, as it is seen, nowadays, as an asset available to intelligence agencies in the knowledge production process for decisionmaking.

Under the new intelligence paradigm, the intelligence agencies have acted in order to develop a framework to manage their relationships with academia, as the academics have what should be considered as the core of the intelligence mission – knowledge (Arcos, 2013).

Like media journalists, academics are among those categories of stakeholders that have the capability to find and interpret information about intelligence developments both in their countries and in other, and thus become key-actors in shaping public opinion, media or even policymakers.

In the context of the openness policies implemented by many intelligence agencies, in the last years, the academic world can provide support for building an accurate public perception of the governmental agencies mission, process and role in defending national strategic interests. Furthermore, the academic world can play a role in providing value as a place to send personnel for obtaining knowledge or expertise or ways to improve intelligence analysis practices.

Human resources in the knowledge society

The present society, where everything is or at least tends to be open, is marked by innovation and a constant reduction of boundaries. Managing uncertainty is a process that intelligence agencies cannot fulfill without qualified human resources.

From this perspective, some experts state that "individual talent is becoming increasingly important in the 21st century. What one knows and can do with their knowledge in different contextual formats drives their employability. In other words, people who can innovate and generate new value with their knowledge will lead employment growth. Those who do not will be replaced by machines, outsourced, or be outmoded by those who can" (Moravec, 2013, p. 10).

Collecting and analyzing information in the abundance of data and sources has become an increasingly difficult task for intelligence practitioners and ensuring new and improved technological means is not enough. The role of technology in human potential development for creative employees (IT&C skills) cannot be denied, but that is not enough for maximizing the process.

More skilled human resources can also be ensured by applying a range of principles, such as improving competencies from different areas of expertise (from history to mathematics or linguistics), constant learning or nonformal analytical processes (critical thinking, imagination, intuition).

As intelligence has become an important part of the academic field, a wide variety of intelligence education programs sprung up, in order to meet the demand for more focused education and training. Also, the literature on teaching intelligence has expanded.

In this context, more and more universities (in countries such as United States, Great Britain, France, Spain or Romania) have developed programs (undergraduate, graduate or postgraduate) dedicated to this field of expertise, with many civilian or military experts as lecturers.

The courses include basic knowledge of intelligence activity – information gathering and analysis, ethics, intelligence activity history, limits of intelligence activity –, as well as more specialized studies – on military operations, terrorism and counterterrorism, counterintelligence, strategic intelligence, business intelligence, foreign policy, organized crime, economy, political sciences, databases management etc. Also, there are courses dedicated to advanced search and analysis methods, creativity, critical thinking or social media.

A relevant case is that of the Office of the Director of National Intelligence, which sponsored the Centers of Academic Excellence Program, in response to the increasing need for Intelligence Community professionals educated and trained with skills, capabilities and knowledge in order to carry out security objectives. Ten universities were part of this program.

In an article published in International Journal of Intelligence and Counterintelligence, Ruben Arcos (2013, p. 332) underlined that "the establishment of intelligence outreach programs and policies in countries like the United States and Canada perhaps best expresses the emergence of a new intelligence approach for facing the threats and challenges of today's dynamic security landscape". In this context, the expert also offered an insight on the results achieved in Spain through the National Intelligence Centre's (CNI) Intelligence Culture Initiative.

In 2005, CNI signed several agreements with Spanish universities, in an attempt to compensate the lack of academic research and programs on intelligence. This initiative led to the rise of university research teams on intelligence and the emergence of a Spanish network of universities and scholars.

The main objectives of this academic initiative were: to make intelligence a discipline for study and research, encouraging its inclusion in university curricula, and leading to research projects on relevant issues; to allow the country's intelligence services to benefit from the knowledge and experience of scholars on relevant issues and matters of interest for intelligence services (Arcos, 2013, p. 341).

Ruben Arcos also noted that "getting the stake of expertise from scholars of many different academic disciplines and areas also requires the stake of understanding by academic scholars of these organizations' mission, support from the government, and a program for educating these publics to effectively obtain the stakes that they hold and that the service seeks, namely expertise" (Arcos, 2013, p. 340).

Key issues: politization and ethics

Transparency is the fundamental principle of democracies and, from this perspective, finding the proper way to communicate to the public opinion what intelligence is, the mission and priorities of an intelligence agency, the services it provides and how it carries out its functions is essential in order to ensure the support of all stakeholders involved in protecting national security. Thus, the process of educating the public about intelligence issues, processes, and functions is very important.

The role that intelligence organizations should play in relation to policy is also a much debated subject. From a theoretical point of view, policymakers and intelligence services need each other: without a receptive audience, any intelligence product would be worthless, but as international politics are characterized by ambiguous data, the secret information provided by intelligence can reduce uncertainty.

It should be stated that there are limits to what "analytical objectivity" really is and the degree to which such thing can be accomplished (the same principle applies to the so-called independence of the analytical process).

Stephen Marrin (2013, pp. 1-4) underlined the wide variety of conceptions related to the degree in which intelligence influence or should influence policy. Thus, intelligence role is regarded either as a limited one – to inform, assess, and/or forecast (the focus in on the production of information and knowledge) – or as part of a more complex interpretation: a support to decision and a means to reduce uncertainty and the incidence of surprise.

A greater distance between intelligence and policy (the traditionalist perspective) may produce a more accurate but less influential product whereas increased closeness (the activist perspective) leads to higher influence but decreased accuracy.

The author advanced a new term used for describing types of politization – analytic politization, that can lead to poor decisions and, as a consequence, to policy failure, as political desires and pressures can push the expert analysis and advice further from the truth (Marrin, 2013a, p. 34).

Stephen Marrin also quotes Gregory Treverton's opinion, according to which politicization can have at least five meanings, which can apply simultaneously: direct pressure from senior policy officials; a "house line" on a particular subject leading to the suppression of alternative interpretations; "cherry picking" - in some cases, senior officials choose their favorites out of a range of assessments; the asking of leading questions or asking questions repeatedly; a common "mindset", whereby intelligence and policy share strong presumptions (Marrin, 2013a, p. 39).

As part of this politization debate, the researchers also focus on the critical issue of trust, in order to ensure the lack of any sign of political abuse or misuse of intelligence. The matter of politization should be weighted for its costs and benefits in terms of achieving policy goals, but there is a thin line between political contamination and presenting intelligence assessments in ways that engage decisionmakers' concerns.

The so-called "political contamination" can be avoided by a strong democratic control over intelligence activity that, according to Amit Steinhart and Kiril Avramov (2013), depends both on a country's history and its constitutional and legal systems, and on the extent of democratic tradition and political culture.

Ensuring the creation of public value and a good public perception on intelligence services' activities and national security matters may prove to be a very difficult task for every intelligence agency, as public opinion is an important intelligence stakeholder. Whereas citizens expect effective protection against vulnerabilities and threats (corruption, terrorism, organized crime etc.), they also want law abiding intelligence activities, conducted with the protection of civil rights and liberties. From this perspective, one of the most important elements that can modify public perception and determine public trust in the intelligence services is the media.

It may be that proper employment of secrecy that serves the public interest, but there have been cases that underlined the limits of openness policies, as national interest is, above all, the main objective of any intelligence agency.

As terrorism and cyber defense are two of the most important threats mentioned in the security strategies drafted and adopted by all developed countries, at least in the last few years, it would have been almost impossible for intelligence practitioners to avoid the debates regarding the issue of ethics or protecting the freedom of speech.

Sir David Omand and Mark Phythian (2013) observe that a decade ago, the literature regarding the relationship between ethics and intelligence was very limited. The post-9/11 world changed both the role of the security agencies – turned into key-players in the war against terrorism –, and the way the public opinion understands security.

Mark Phythian notes ”many ethical dilemmas that face intelligence professionals, agencies, and governments arise from a simple fact: national intelligence agencies are precisely that – national”, meaning that “their responsibilities and obligations are defined by reference to the state for which they are an information-gathering and early-warning arm” (Omand and Phythian, 2013).

The results of many opinion polls conducted in recent years regarding the task of ensuring national security conducted by governmental agencies have shown citizens trust their governments and sometimes even approve the methods used in order to ensure their safety. But beyond this trust (more or less reliable), intelligence services must still prove in every instance their practices are consistent with national law and ethics.

The recent debates regarding the highly classified electronic surveillance program developed by the National Security Agency may be considered from the perspective of what Mark Phythian called “social acceptability” (Omand and Phythian, 2013, p. 44), which means that “to be able to demonstrate, or argue with a degree of plausibility, that something is legal impacts on the way people come to view it”.

As some experts observed, the first reactions to the reports revealing the NSA program were that “it killed trust in web freedom” and “it threatened individuals’ online privacy” (Cheong, 2013). This kind of perspective takes us back to some of the questions mentioned before regarding transparency and accountability, but it leaves out the relevance issue – also essential for democratic governance, but less important in this context.

It is a well-known fact that the Internet and social media have become the main medium of communication for non-state actors. And indeed, the authorities can always reassure the public opinion that their programs were or are used for valid foreign intelligence purpose.

Yet a brief or commonly accepted justification or explanation would be almost impossible to provide, as it would be ensuring a balance between privacy/human rights and national security concerns.

Conclusions

A “synchronization” of intelligence theorists and practitioners’ priorities is possible, but not in the near future.

The first usually seek to correlate social and organizational change and issues, such as improving analytical methods, and the nature and role of intelligence studies are very important.

The latter, although very much concerned about the same issues mentioned before, will always be mostly preoccupied with detecting risks and threats so as to ensure national security.

References:

1. Arcos, Ruben, (2013), *Academics as Strategic Stakeholders of Intelligence Organizations: A View from Spain*, in International Journal of Intelligence and CounterIntelligence, vol. 26.
2. Brizga, Sandra, Patricia Geraghty, (2011), *Strategic Framework for Integrated Natural Resource Knowledge Management*, Victorian Catchment Management Council, accessed on July 20, 2013 at www.vcmc.vic.gov.au/PDF/FrameworkKnowledgeManagement.pdf.
3. Cheong, Damien D., (June 24, 2013), *Intelligence-Gathering in the Digital Age: Building Trust in PRISM?*, in *RSIS Commentaries*, no.115/2013, S. Rajaratnam School of International Studies, accessed on August 16, 2013 at www.rsis.edu.sg/publications/Perspective/RSIS1152013.pdf.
4. Crompton, Helen, (2002), *Knowledge Production and Management in the 21st Century*, Manchester Metropolitan University Business School Working Paper Series Online, accessed on August 20, 2013 at www.ribm.mmu.ac.uk/wps/papers/03-02.pdf.
5. Hoppe, Magnus, (2013), *The intelligence Worker as A Knowledge Activist - An Alternative View on Intelligence by the Use of Burke’s Pentad*, in *Journal of Intelligence Studies in Business 1*, accessed on May 29, 2013 at https://ojs.hh.se/index.php/JISIB/article/download/57/63.
6. Johnson, Loch K., Shelton, Allison M., (2013), *Thoughts on the State of Intelligence Studies: A Survey Report*, in *Intelligence and National Security*, vol. 28, no. 1, 2013.
7. Lahneman, W. J., (2003), *Outsourcing the IC’s stovepipes*, in *International Journal of Intelligence and CounterIntelligence*, nr. 16, 2003.
8. Marrin, Stephen, (2013), *Revisiting Intelligence and Policy: Problems with Politicization and Receptivity*, in *Intelligence and National Security*, vol. 28, no. 1, 2013.
9. Marrin, Stephen, (2013), *Rethinking Analytic Politization*, in *Intelligence and National Security*, vol. 28, no.1, 2013.
10. Moravec, John (ed.), (2013), *Knowmad Society*, in Minneapolis: Education Futures LLC, accessed on May 19, 2013 at http://www.knowmadsociety.com.

11. Sir Omand, David, Phythian, Mark, (2013), *Ethics and Intelligence: A Debate*, in *International Journal of Intelligence and Counterintelligence*, vol. 26, no. 1, 2013.
12. Rovner, Joshua, (2013), *Intelligence in the Twitter Age*, in *International Journal of Intelligence and CounterIntelligence*, vol. 26, 2013.
13. Steinhart Amit, Avramov, Kiril, (2013), I*s Everything Personal?: Political Leaders and Intelligence Organizations: A Typology*, in *International Journal of Intelligence and Counterintelligence*, vol. 26, March 2013.

INTELLIGENCE CYCLE MODEL DILEMMAS AND SOLUTIONS

Mircea MOCANU*

Motto:
"Of all the weaknesses of the Cold War intelligence paradigm, the hegemony of the intelligence cycle models probably the most important single factor in producing an intellectually inadequate concept of intelligence"
(Wilhelm Agrell, 2009)

Abstract

A result of the pressure put by globalisation and the Information Age on all informational processses, various sugestions to adapt the intelligence cycle range from slightly amending the model to radical change. This paper supports an adaptation of the cycle, and gets inspiration from communication theory, where the receiver of the communication is, of course, part of this process. The decision taken by the beneficiary and the subsequent actions take place in the risk management system, above the intelligence system. So, intelligence operates as an open system, and Dissemination seems to be the weakest link of the cycle. Complexity theory issues and the Clausewitzian friction are also considered. This paper proposes Utilisation as a main link of the cycle, instead of Dissemination and discusses the consequences, variations of the model, and the implications in intelligence management.

Keywords: intelligence cycle, intelligence management, communication process, open system, dissemination, decision-making.

The informational cycle model in a complex environment

Since the last decades of the XX Century, the major transformations generated by the Information Age impact upon any human activity involving the use of data and information, from journalism to business, from public services or education to intelligence services.

* PhD retired from the Romanian Armed Forces in 2013 as head of analysis in the Military Intelligence Directorate. This paper draws from the author's volum *Intelligence from Networks to Decision and Action*, Bucharest: National Defence University „Carol I", 2014.

The functional pressure generated by globalisation and technological progress on all informational processes reveal the need for a critical evaluation of the informational cycle as afunctional model defining the heartbeat in all the fields operating with information. From the point of view of complexity theory, the above mentioned functional pressures reflect more intense and quicker interactions among the actors within the informational environment. They also reflect an increase in the entropy an the strengthening of the non-linear feature of all phenomena, described by the well-known "butterfly effect": a minor change in a distant part of the system causes a significant change in the opposite side of the system. In a *complex system*, the disproportionate effects give away only a blurry causality, and a quicker pace of all information processes is needed for understanding and controlling such causalities.

Current global phenomena produce deeper implications especially upon the decisional system and the metabolism of the organisation or macro-systems associated to power writ large, because power relations are the most sensitive to the impact of new information technologies (Marguin, 2001, p. 120). Thus, an in-depth research into the fine grain and the intimate links of the informational cycle look like a promise path for the critical domains, with major social impact, such as media, economy, education, national security, and law enforcement.

Yet, what is the informational process? In a nutshell, information of any kind needs to be obtained, processed – more or less – and the result is used one way or another. Considering the system as a black box, the information has to enter from the environment into the box, where the system processes them in a certain way, then the system does something as a result of the absorbtion of that information: it moves, or it changes colour, or it signs an international treaty. The use of information, basically for decision-making and subsequent actions, generate, the need for new information to continue and deepen the process of knowledge in view to further a pursued interest. Inside the black box, as a result of input information processing, somebody produce another information, and passe it to somebody else, who decide, for example, to sign the international treaty.

In terms of complexity theory, as a consequence of that decision, *the info-decisional system*, perceiving a certain *criticality*, triggered an action/ *transition,* which changed its *state* (status) within the environment. In a new situation then, the system needs new information to decide the way to *interact* (what to do) in the new *state*, how to control the new *criticality*.

Considering just the information, so only the informational (sub-) system within the black box, not the decision or the action, the loop ends and, in the same time, starts again, on another level of knowledge, hence the 3D spiral image of the informational cycle, in an iterative view. These three phases are the core of the informational process, because they are the ones operating directly with the information: *obtaining* information, *processing* it, then *transmitting* the information to a decision-maker (who uses it for starting an action).

However, the complexity of the intelligence activities points to other more or less important operations, eligible to be added to the core triade of the process mentioned above (obtaining/collection/access, processing/ analysis, and distribution of information). The most important case includes command, control, direction, development and planning of the whole work, as well as orientation and prioritization of all activities pertaining to the other separate phases of the informational cycle, and for the entire information process as a whole. This functional component is included in most representations of the informational processes, usually under the name of *Direction*.

Consequently, the classic form of the informational cycle has four phases: *Direction – Collection – Analysis – Dissemination*, as the model in Figure 1 shows.

In business, the effects of modern global communications were obvious, mainly in stock markets. Then, in the field of security, the effects of the Information Age upon the informational cycle was felt primarily in military operations, as the battle rhythm accelerated the pace of changes, especially in the case of non-conventional conflicts[1]. These conflicts were the first show of complexity at revolutionary scale in military affairs, considering *asymmetry* as expresion of *non-linear bahaviour*.

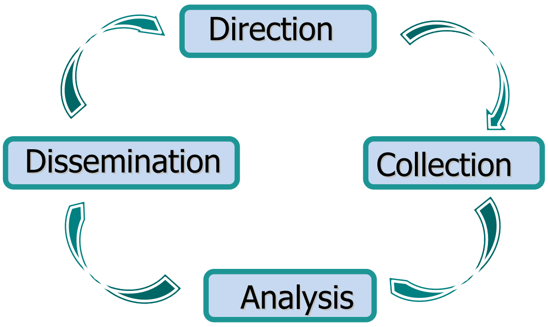


Figure 1. The classic model of the informational cycle

Besides the basic form shown in Figure 1, there are several other graphic representations of the informational cycle model, featuring the above mentioned considerations and using different terms for different process phases. Some models are more sophisticated and display secondary transfers to reflect various functions specific to intelligence

[1] The term "non-conventional" is also used, in this paper, equivalent to "assymetric" and "transnational".

activities. For example, in some models, *Processing* appears as a phase of its own, separated from Analysis, because it includes a large number of activities[2] meant to bring collected information to a shape which can be used by the analysts.

In the particular domain of intelligence, the informational cycle is termed «intelligence cycle» to underline the secret information component and the specific activities of the intelligence process. Similarly, the term "intelligence support" defines the component of the general *information support* (with information of all kinds) provided to decision-maker, for the particular case of intelligence (mainly, involving secret information).

Critics and amends to the classic model of the intelligence cycle

The limits of the intelligence cycle classic model have been underlined by many experts of the realm, pointing to major failures in reflecting several important activities in intelligence services practice and the new security realities which request either interleaving or omission of core phases.

Kristan Wheaton (2011) builds a true indictment against the intelligence cycle classic model, which he deems "a relic of the Second World War", the cause for resource waste and an obstacle to progress in intelligence, because the intended reforms would engage the intelligence services on wrong directions, should they be based on a flawed model (Wheaton, 2011, pp. 1-2). K. Wheaton objects that the traditional model is linear and sequential, while the process it is supposed to represent is non-linear, interactive, simultaneous, collaborative and iterative, especially in the conditions of the global asymmetric threats. He notes that the human mind does not operate in a linear manner either, and indentifes two directions where the efforts are engaged to reflect today's intelligence process, i.e. tweaking the model to better reflect the reality, respectively to overhaul the graphic representation of the way the intelligence services work (Wheaton, 2011, pp. 5-7).

The most radical visions presented by K. Wheaton are the *sensemaking loop* developed by Peter Pirolli and Stuart Card, and the *Target Centric Approach* (TCA) imagined by Robert Clark.

Pirolli and Stuart developed (2006) a chain of five succesive loops of actions which include, in principle, elements and activities belonging to the the phases of collection, analysis and dissemination, as they appear in the classic cycle. The process starts with "external data sourses" and the feed-back

[2] For example, decryption, translation, imagery interpretation, even transportation to the analyst, as well as tagging and labeling for the convenience of all branches in the intelligence structure.

appears in each loop, but the whole process is still linear, like stretching the classic cycle broken after Dissemination, limited here to the act of "presentation". In the struggle to represent truly more concrete activities, the sensemaking loop model introduces new concepts, gets complicated and does not solve the limitations of the classic cycle. Even worse, there is no reference to beneficiaries and requirements, and no general feed-back, the cyclic pattern of the intelligence activity being ignored.

The more recent TCA model (2009) is more successful because it responds very well to the intelligence activity in military campaigns, where the effort of the entire organisation can focus on a single target. More precisely, R. Clark (2009) develops a graphic model in which two loops are tangent in the point represented by the objective of the intelligence structure (the "target") and embodies the keen requirement to integrate the activities of analysts and collectors. The very merit of this model is also drawback, i.e. the fact that it cannot be applied *in extenso* to large organisations, which deal with events, crises and conflicts all around the World, including transnational risks and threats.

K. Wheaton comes up with his own suggestion for a representation of the intelligence process in the form of four parallel and partially overlapping waves, but also presenting succesive surges, which reflect the dominant activity at a certain time. These waves are the *mental modeling*, *collection*, *analysis, and production*, with no reference to dissemination or user.

The models proposing only the revision of the classic cycle either suggest the inclusion of the user in the model (Lisa Krizan, 1999 and Gregory Treverton, 2003), or rename collection by the larger term of "access" (Sir David Omand, *Securing the State*, 2010). Others describe the process in multilayer representation (Lowenthal, 2005) or extensively detail the known activities (Johnson, 2005).

A possible way out

"Most intelligence professionals see the intelligence cycle as «imperfect», but generally the best available description of [a complex and dynamic] process, and useful for teaching broad concepts" (Wheaton, 2011, p. 1) of the intelligence activities. However, "the cycle is a simplification – possibly an oversimplification – and real-world intelligence has to be understood in terms of a far more complex ad-hoc model" (Agrell, 2009, p. 108) than the established picture of the intelligence cycle.

Among the flaws, K.Wheaton (2011, pp. 3 and 5) thinks that „the simplicity of the cycle is both seductive and deceiving", but admits that its

„continued existence suggests that its inconsistencies are outweighed, to some extent, by its simplicity". However, the simplicity and natural construction of the conceptual model in discussion provides generality, flexibility, and strength to the paradigm which all informational architectures and all activities dealing with information are based upon. This is why I support the „tweaking" of the intelligence cycle to present realities, and not an „overhaul" or discarding the classic cycle, which still offers two essential features in a concise form: it presents logical action steps, and reflects the cyclic and iterative character of the intelligence process.

The weakest link of the model, the area most susceptible to be examined with priority, seems to be dissemination, the finalization of intelligence support.

Why? The perennial issue of the functional distance between the intelligence structure and the decision-makers draws attention to the positioning of the whole intelligence system *vis-à-vis* the superior/above system, which is the decision-making system. Thus, the intelligence support is located within a larger function, that of *risk management*, albeit in national security, law enforcement or business. In the same time, the practical destination of the intelligence products – the integration of the "actionable" information (included in these products) into decision and concrete action – highlights the importance of the functional relation between the activities in the intelligence domain and the realities in economy, national security or law enforcement.

The interaction between the intelligence structure and the decision-making system is done through two points of the intelligence cycle, one for the transfer of the intelligence *requests* and that of the beneficiary *feed-back*, and the other for *dissemination* – the completion of intelligence support.

These two moments of the intelligence activity are considered to be the most tricky. This statement is based on the fact that these "gates" are the contact points with the decision-making system, where the rubber meets the road, while the other activities in the intelligence cycle occur **inside** the intelligence structure, more stable and strongly regulated. Therefore, they benefit from the coherence of a stronger self-correcting validated system.

The two "gates" of the intelligence cycle which mark the intake – exit of information into/out of the intelligence organisation prove that intelligence is an *open system*. The intelligence cycle defines the information flow which crosses both the intelligence structure and external compartments, belonging to the beneficiary. The model presented in Figure 2 highlights the open system feature of the intelligence structures.

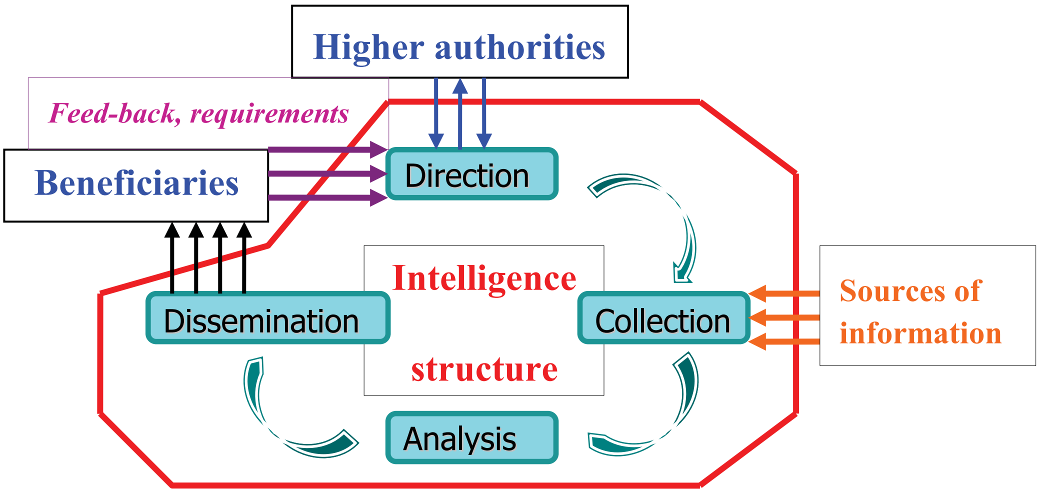


Figure 2. Communication gates between the intelligence structure and the environment

Figure 2 also shows other interactions with the environment: the relations with chain-of-command authorities (in administrative capacity, not as beneficiaries) and the injection of information into the intelligence flow. These interactions support the idea of open system, and the complex interactions within the security environment, but present no further interest for this paper.

Studies about the classic phases of the intelligence cycle do not clear out the destiny of the information after dissemination of the intelligence products to the beneficiaries, although some vaguely maintain the *user* or the *integration / consumption* of intelligence, following *dissemination*. There are studies about the distance between analyst and decision-maker, the importance of the feed-back and the actions conducted as result of the inelligence support. However, the transfer towards the beneficiary "beyond the regiment gate" has not been examined in-depth, nor has the contents of the phase called "*dissemination*" seen as *intelligence support*, not as *delivery*, or the processes lived by the information after its transfer to decision-maker and the feed-back "chemstry".

Regarding dissemination, research on the intelligence support as *communication process* provide significant conclusions about the rapport between the intelligence structure and the beneficiary of intelligence work. The revision of this functional rapport is relevant under Information Age pressure and networked operation (networks of distributed capabilities). However, in today's military science, "the concept of Network Centric Warfare (NCW) is wrought around (...) the term of information dissemination" (Dumitru and Roncea, 2005, p. 41). The role of dissemination and the traditional format of the intelligence cycle reflect a *closed system* approach on intelligence structures, and ending the intelligence cycle loop by the phase called *dissemination* reveals a reasoning jam and a parochial vision on the intelligence domain. Such drawbacks are caused by the institutional responsibilities of the intelligence services developed in the Industrial Age and especially during the Cold War. Nontheless, "the process of transfering information from producers to consumers is largely standardized. The intelligence community established a «production line» which covers the types of products and the beneficiaries it has to serve" (Lowenthal, 2005, p. 48). By this «product delivery», the duty of the intelligence service is deemed accomplished.

I believe, though, that the way intelligence is integrated into the *decision* taken by the beneficiary and into the *action* based on that decision provides important conclusions about the very structure of the intelligence cycle, opening the gates towards the optimization of intelligence activity as a top driver for national security, as well as for the other major application domains – business or law enforcement.

Following the increase in the intensity (clausewitzian friction) of the confrontation, albeit a military, economic or law enforcement conflict, in the conditions of distribuited capability operation (in network), the intelligence support displays certain particularities which generate significant mutations not only on management requirements in intelligence, but also, again, on the core phases of the intelligence cycle.

Proposal for improving the classic model of the intelligence cycle

Noting that the decision-makers play a significant role in all phases of the intelligence process, seems logical to drop the limitation of the intelligence cycle to activities performed by intelligence structures. Thus, failing to include the beneficiaries into the intelligence cycle looks like a judgement error, especially in the conditions of modern technologies and non-conventional threats. In the same time, looking at the intelligence support as a *communication process*, having the receiver of the communication inside a model of the process is mandatory, as the scholars of the Palo Alto School[3] argued. They introduced a *psychosocial/interactionist model* of the communication process, presented in Figure 3, to include the *psychological determinants* of the communication process actors.

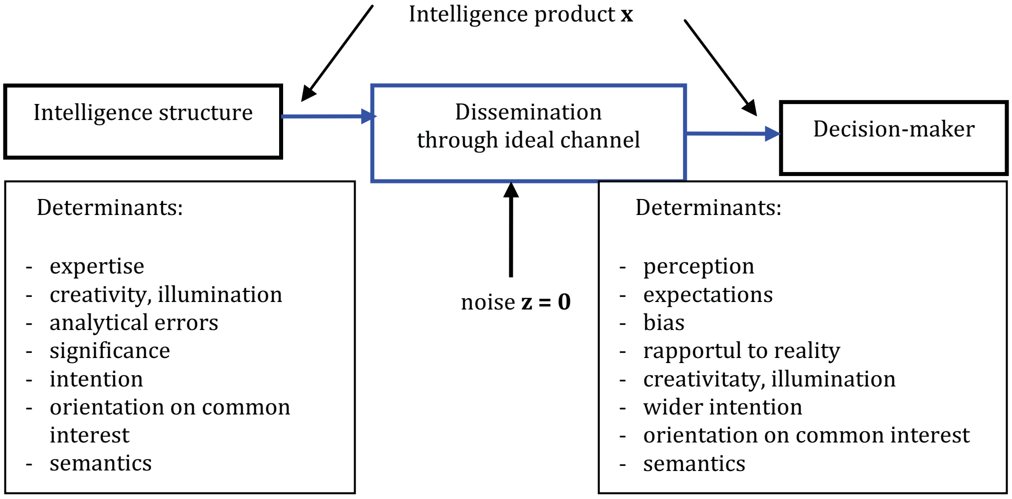


Figure 3. The interactionist model of the informational process
(source Sălăvăstru, 2004, pp. 116-117)

As the trigger of decisions which are the very *objective* of intelligence support, the beneficiary ought to be considered a natural actor of the intelligence cycle, as Greg Treverton suggests. Consequently, a model of the intelligence cycle which reflects the roles of the main actors: *director* - *collector* - *analyst* - *beneficiary* seems quite natural.

The decision-maker activity in rapport to intelligence products can be termed as *use* or *utilization,* which has been proposed before as part of the cycle, but has not been developed as a concept. Based on the functions of

[3] Group of researchers of various domains (sociologists, linguists, psychiatrists, antropologists) reunited around Gregory Bateson. The Palo Alto School (Stanford University) includes Donald Jackson, Paul Watzlawick, Janet Beavin, Edward Hall, Ray Birdwhistell, Erving Goffman, Margaret Mead, Virginia Satir, Jay Haley, John Weakland, Richard Fish *et. al.*

communication processes, I can argue that intelligence utilization implements three functional categories of intelligence support: *construction of intelligence superiority*, *warning*, and *integration into action* (Mocanu, 2014). These functional categories reflect different levels of clausewitzian friction, different levels of impact by the actionable substance transfered through intelligence products, as well as different approaches to the international environment complexity in security, economy or law enforcement.

The above rationale supports the general conclusion that *the use of intelligence products* by their integration into decision and subsequent action *is a natural component of the intelligence cycle*, following the dissemination procedure, and closes the cycle logically, by beneficiary's requirements and feed-back, towards the phase of direction. In the proposed model, presented in Figure 4, *dissemination appears as a procedure linking two main phases and not a phase itself,* is the conection between analysis and utilization, *and not an essential phase* of the intelligence cycle.

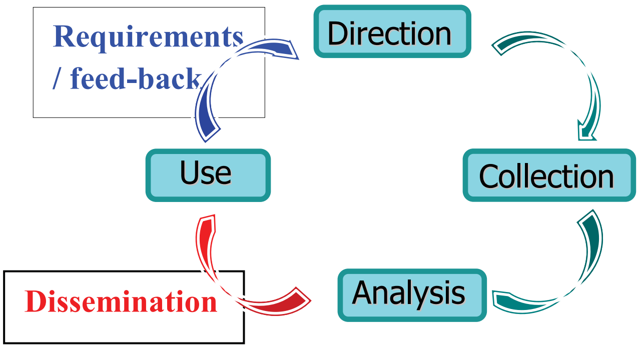


Figure 4. Proposed model for the intelligence cycle

In the same time, the proposed model allows developments in defining the levels of feed-back (*analytical*, *system*, and *phenomenon*) (Mocanu, 2014) and the study of intelligence requirements according to the type of intelligence product utilization. The feed-back occurs also through an interaction gate towards outside the intelligence system. Consequently, it completes the natural cyclic of the model.

Conceptual developments of the proposed model

Enriching the proposed model with detailed activities is easy. Interesting, however, is the direction to further simplify the model, aiming to generalise and streamline the intelligence process. For an ever simpler form of the intelligence cycle, the *utilization* phase should not be the first shed from the loop, but probably the *direction* phase. The reason is that direction is not crossed by information for more than validation before dissemination. Since it applies to all phases of the cycle, by chain-of-command coordination, direction can be placed in the centre of the cycle, as shown in Figure 5. By the spokes of the cycle, from the centre to the three remaining phases of the cycle, this model reveals the direct connection of Direction to all main intelligence activities, the responsibility for dedicated management of the structures performing the three main phases of the process: *Collection, Analysis, and Utilization*.

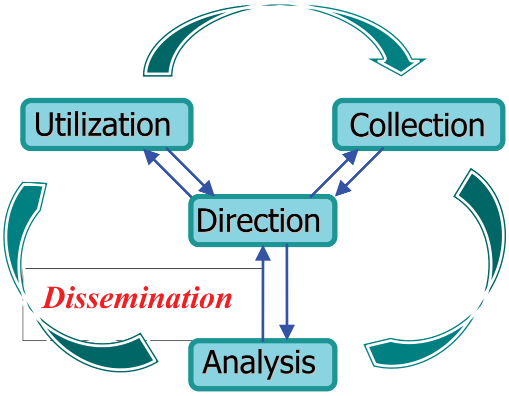


Figure 5. Intelligence cycle with central direction

The inclusion of *Utilization* as an essential phase of the intelligence cycle provides conceptual avenues for developments in the management of intelligence structures aiming to improve intelligence support. By considering *use/utilization* a phase of the intelligence cycle, the intelligence structures can shape intelligence support in its entirety, bearing in mind the three identified functional cathegories. The proposed model can thus be completed in versions to include specialised management structures: collection management (CCIRM[4]), production management, and intelligence product *utilization management*. This third structure would take over the responsibilities regarding dissemination, cooperation, and the absorbtion of the feed-back, but also improves the intelligence support by an *intelligence product utilization policy*.

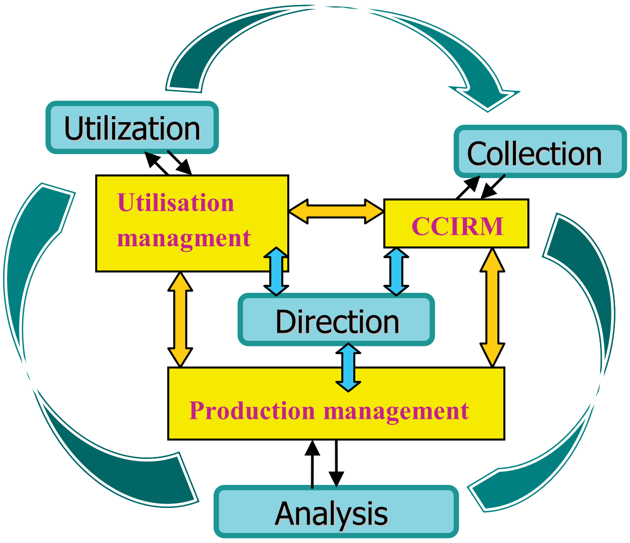


Figure 6. Intelligence cycle with specialized management

The management activities corresponding to the three core phases of the intelligence cycle can be represented as a crown around the central direction box. Such model, presented in Figure 6, highlights the horizontal cooperation among the manage-ment compartments dealing with specific intelligence issues.

[4] CCIRM – Collection Coordination and Intelligence Requirements Management.

The management activities corresponding to the three core phases of the intelligence cycle can be represented as a crown around the central direction box. Such model, presented in Figure 6, highlights the horizontal cooperation among the manage-ment compartments dealing with specific intelligence issues.

This model can also be represented in 3D (Figure 7), as a cone where the loop of essential three phases forms the directrix (the cone's circular basis), Direction is the vertex (tip of the cone), and the three kinds of specialised management form a median circle. This model suggests better the spiral dynamics of the intelligence process.

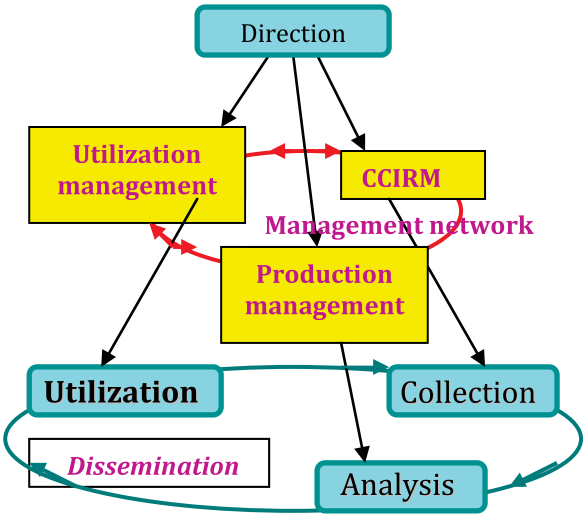


Figure 7. Conic model of the intelligence cvcle

Conclusion

The study of the intelligence cycle and the efforts to identify new conceptual solutions to better serve the adaptation of the intelligence services to current realities of the security environment are in full swing.

In the versions proposed in these pages, the new model of the intelligence cycle, which includes utilisation as an essential phase instead of dissemination, opens avenues for the optimization of the use of intelligence capabilities and the improvement of intelligence support by taking into account all aspects of risk management in their entirety and complexity.

References:

1. Clark, Robert, (2009), *Intelligence Analysis: A Target Centric Approach*, Congressional Quarterly Press, Washington DC.
2. Cristea, Dumitru, Ion Roceanu, (2005), *Războiul bazat pe reţea. Provocarea erei informaţionale în spaţiul de luptă*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti.

3. Lowenthal, Mark, (2005), *Intelligence. From Secrets to Policy*, CQ Press, Washington DC.
4. Marguin, Jean, (2001), *Tehnologia informaţiei va schimba lumea?*, în *Puteri şi influenţe*, Editura Corint, Bucureşti.
5. Mocanu, Mircea, (2014), *Intelligence de la reţele la decizie şi acţiune,* Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti.
6. Pirolli, Peter, Card, Stuart, (2006), *The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis*, PARC paper, accesibil la www.vadl.cc.gatech.edu/taxonomy/docInfo.
7. Sălăvăstru, Dorina, (2004), *Psihologia educaţiei*, seria Collegium. Psihologie, Editura Polirom.
8. Treverton, Gregory, Agrell, Wilhelm (coord.), (2009), *National Intelligence Systems. Current Research and Future Prospects*, Cambridge University Press.
9. Wheaton, Kristan J., (2011), *Let's Kill The Intelligence Cycle*, accesibil la www.sourcesandmethods.blogspot.com/2012/03/part-13-whole-picture-lets-kill.html.

OSINT

THE EMERGENCE OF SOCIAL MEDIA INTELLIGENCE

Rareş-Adrian RAICU[*]

MOTTO:
"There are three kinds of intelligence: one kind understands things for itself, the other appreciates what others can understand, the third understands neither for itself nor through others. This first kind is excellent, the second good, and the third kind useless."
(Niccolo Machiavelli)

Abstract

In a world of constant change and with an environment of transnational security which varies depending on the fluctuations of international reality, intelligence is undergoing a series of mutations focused on a new typology of vulnerabilities, risks and threats to national, regional and international security. At the beginning of the millennium, the stages of globalization leave a prominent mark on society, as well as accelerate developments of information technology and science. All these are meant to facilitate the transition from the industrial age to the informational era and then to the knowledge society. In this context, asymmetric threats have diversified, both in number and intensity. Recent developments in technology and the shift from industrial society to the information society facilitated the dissemination means of these threats. Intelligence has been forced to adjust to the new requirements of the security environment and to develop new ways and methods to counter modern threats and risks.

Keywords: social media intelligence, modern threats and risks, informational era, knowledge society.

Introduction

In a world of constant change and with an environment of transnational security which varies depending on the fluctuations of international reality, intelligence is undergoing a series of mutations focused on a new typology of vulnerabilities, risks and threats to national, regional and international security. At the beginning of the millennium, the

[*] Romanian Intelligence Service.

stages of globalization leave a prominent mark on society, as well as accelerate developments of information technology and science. All these meant to facilitate the transition from the industrial age to the informational era and then to the knowledge society. «*The expansion of the virtual world led to the emergence of a new dimension of state power, "the digital power", with long term effects on strategic knowledge and on the state actions both national and international speaking. Also, the individual has acquired new tools, through access to databases and networks, tools that can influence directly the exercise of power, domestically or internationally. The recurrence of "Facebook" and "Twitter" revolutions form Europe to Middle East demonstrates the impact of these virtual instruments on the political regions, an impact that was unimaginable less than a decade ago. Evolving forms of "digital power" will represent, equally, development opportunities, but also vulnerabilities and security challenges, and their management will be determined by the ability to access, detect and use information*» (Maior, 2011, p. 2).

In this context, asymmetric threats have diversified, both in number and intensity. Developments in technology and the shift from industrial society to information society facilitated the increase in the dissemination means of these threats, intelligence being forced to adjust to the new requirements of the security environment and to develop new ways and methods to counter modern threats and risks.

The interpenetration and coexistence of some elements belonging to the informational era with the layer of the new knowledge society creates the current world context, at the beginning of the XXIst century. In this context, one can speak about a permanent necessity to adapt the specific intelligence activity to the new types of challenges, risks and emerging threats of the knowledge society and of those related to the informational era, characterized by dynamism and unpredictability. Today, information technologies are developing at a rapid rate, being disseminated faster and often not being used for creating a favorable security climate. The expansion of asymmetric threats, mentioned above, materialized in the form of terrorist or extremist groups or, more recently, as modern cyber threat uses all the benefits that the informational society can offer. Thereby, if until now one could speak, for example about a conventional terrorist spread rapidly by globalization and which could be materialized by exploiting national and international security breaches especially in the physical space, today one can speak about terrorism adapted to the new challenges of the informational era and especially to those knowledge societies that are fully exploiting the virtual opportunities.

Therefore, intelligence should be conceptualized and directed to a collection of data and information from all available sources, whether clandestine or public. The opening of intelligence and security services to the civilian sector and the exponential growth of OSINT usage, without neglecting the HUMINT (Lesidrenska & Bancheva, 2014, p. 151) element and the other INT's, be it the MASINT, SIGINT, IMINT or even the specific means and methods of intelligence can guarantee intelligence services success in preventing and countering risks and threats to the knowledge society.

As mentioned earlier, the emergence of informational and communicational technologies also attracted, apart from opportunities, a number of vulnerabilities that by materialization and manifestation could seriously damage the international security climate. However, the rapid evolution of the phenomenon of social media and the current societal trend towards interaction and communication, due to the existence of online facilities has led some groups to act, not only in the tangible reality but also in the virtual sphere. So, through their assumed missions, namely to prevent and combat the risks and threats, on the one hand, and to promote and preserve national values, on the other hand, it was incumbent on the intelligence services to direct their activity also to this space, which had not been considered relevant until 9/11. This was a milestone start in understanding the effects of the virtual world on reality.

The starting point of the need to approach the phenomenon of social media is actually the summer of 2011, specifically on August 6. In London, significant street violence emerged with a powerful social impact. The population's grievances began with the shooting of Mark Duggan, a black Tottenham resident, in north London, by a police officer trying to arrest him. Although the reason for his arrest was not made public, many assumed that it was part of an operation of the Metropolitan Police, called *Trident*, which was investigating illegal possession of weapons and their use in drug trafficking or crimes by black minority in England. In the following days, social discontent spread throughout London taking various forms, mostly demonstrations against Great Britain's police structures. Further, as in the case of most demonstrations or protests, social discontent (Le Bon, 2012) transformed in vandalism and theft (Philips, Frost, Singleton, 2012, p. 1).

After Mark Duggan's assassination by the British police, a series of assumptions about his death began to spread in the black community, generating greater tensions that escalated quickly. If initially one could speak about a protest of a group of 200 people who asked for explanations about the man's death, soon things became complicated. Speculations about Duggan's death diversified. In this regard, there were a series of speculations that he was killed intentionally by the policeman who arrested him and that he was shot in the chest after being handcuffed. Another speculation regarded that he would have told his friends 15 minutes before his death that he was surrounded by police, but he was safe (Lewis, 7 august 2011). The uncertainty about Mark Duggan's death was what actually created discontent among the protesters. Thus, they were accusing the Metropolitan Police that no shootout had occurred, that the man did not have a gun in his possession, and that his murder was against the law. Police reports would have indicated that he was carrying a gun, which was acquired even before being arrested from Kevin Hutchinson-Foster. The interrogations and the trials of the latter could not demonstrate and prove the charge. On January 8th, 2014 a verdict was reached that the death of Mark Duggan had not represented a violation of the law (*Mark Duggan inquest and reaction*, BBC News).

As has been noted, the protests began amid these uncertainties and based on the English black community's dissatisfaction. If, at first they spoke about a peaceful protest on the night of August 7th, 2011, the protests degenerated and created violence and tension. So, some questions appeared related to the speed of transformation of a peaceful protest, low as location and number of participants, into violent and widespread demonstrations. Initially the causes of protest's degeneration have been identified in the way the events were presented in the local press and TV stations with national coverage. *On the one hand everything was blamed on local media, and on the other hand on the UK's television.* However what customized the violence in London was the massive promotion of the social media phenomenon.

In this regard, on the social network Facebook, protesters began to create various groups, under different names (*Justice For Mark Duggan and Those Killed by Police*, *Justice for Mark Duggan aka Starrish Mark.Sho! Sho*, *R.I.P Mark Duggan* or *Justice for Mark Duggan*), online communities that expanded rapidly after the beginning of the protests. Some of them even reached 34.841 members (*Pagina oficială de facebook R.I.P. Mark Duggan*). Although more such groups appeared, all turned their attention to the same kind of content. Group managers asked supporters to take to the streets and to demand justice for Mark Duggan. Examples of postings on this (user Shannon Loch: *Screw Police Brutality* or user Milad Gh.: *Hey guys come on…I waiting for YOU! Are YOU with me?*) used generally more biased language, often accompanied by obscene words against the police or against what happened. Most posts on the Facebook social network aimed mainly, besides blaming what happened especially on London Police. These gathered a large number of supporters who were willing to take to the streets and participate in protests as seen in Milad Gh's post.

After more than three and a half years since Mark Duggan's death and since the bloody riots from England, these pages have not completed their activity and their managers continue posting messages against police and seeking solidarity for those killed by police officers *(The Police are the biggest Mafia, but only in this case in a uniform. Fact! BirminghamStrong Justice 4 ALL*

Justice For Mark Duggan aka Starrish Mark.Sho!Sho Stephen Lawrence Charitable Trust Campaign for Justice for Smiley Culture). Moreover, they frequently express their dissatisfaction with the events that happened. During the trial of Kevin Hutchinson-Foster, they asked people again to go out in the streets and support Mark Duggan's cause (*Judgement Day 2013! Let's make it big! Look on the post below for more info. Let's do this 1 time! March 15 at 1:00pm* or *Who coming Birmingham today for demo? Admin Tommy D, Plan B*). The offensive force of the online community in supporting and defending Mark Duggan could be observed on Facebook. Some persons were informal virtual leaders, had a specific coded language, and even promoted multimedia content to instigate and attract as many protesters taking part in violence. Thus, it was easy for them to find about the place and time of the violence from social media.

In addition to using the Facebook app, protesters resorted to exploiting the social media platform Twitter and to making their voices heard in support of Mark Duggan's cause. Through tweets, users of this network managed to quickly spread information, taking advantage of the idea of Internet SMS and all its benefits. Thus, through short messages, they quickly changed dates, particularly about the time and place of the protests and also messages requesting the arrival of a large number of protesters. An example of this can be the user's tweet @carboia, stating *Spoke to them. They're on their way. Be with you soon*, referring to the reunion of all protesters.

Differently from messages of calling supporters and protesters, Twitter's was also used, in the case of the riots that took place in London, as a vehicle of social media propaganda. In the days between 6th and 11th of August a series of rumors about the social dissatisfaction of the community and the forms that their protests took spread as Twitter posts. Tweets of users who claimed that protesters attacked London Zoo and managed to release the animals emerged. So @Twiggy_Garcia, a Twitter user which had 5.178 supporters, was the first that spread the rumors on the platform that protesters entered the zoo and freed all animals. This information appeared also with Twitter hashtag #LondonRiots. At 2 am on August 7th, the user @Deadfreaks spread some information that the riots escalated, and the protesters even managed to enter the fast-food chain restaurants McDonald's and cook their own food, rumor that appears with hashtag #Tottenham. In the same hashtag, @DeclanJMN provided some information which referred to the fact that a 16-year-old girl would have been beaten by London's police, which would have fueled even more the tensions and social discontent. Things went much further, and @andzadio posts within hashtags #LondonRiots, #Londonriot and #Prayforlondon disseminated images with the London Eye in flames, and the tweet was quickly assumed and easily spread, tightening the state of uncertainty and tension among population. Another example of this, is that @jazz_kaur spreads, using #Londonriots and #birminghamriots, a rumor according to which the protesters are leading to Birmingham Children's Hospital (*The Guardian*, December 7, 2011).

However, all the rumors promoted by the aforementioned users through Twitter proved to be false, and ultimately denied even by the London police. All this information had clearly meant to create panic and tension among the population, who did not know exactly what was happening. Protesters used all these rumors to be able to promote their violent actions and gain image before the rest of the community, thus spreading chaos and, worst, tension.

Therefore, available information from Facebook and rumors spread through Twitter proved a possible tension that could extend across UK. Within days, things degenerated in social media. From simple posts related to the death of Mark Duggan and from the desire to avenge his killing, posts that showed violent intentions or massive community organization to express their intentions clearly and complaints against police emerged. Thus everything basically turned into a street riot, built out of violence, theft and conflicts that resulted in casualties.

After the dispelling of tensions and the calming down of both the protesters and their adversity to police and the calming down of the street riots, the Metropolitan Police reported that it was taken by surprise by the emergence of the social media phenomenon and they did not presume that carrying out intelligence in this virtual space, with everything that it implies, from collection and verification to analysis and integration, could have helped officers prevent and counteract the violent actions of protest. Thus, the need and the opportunity to create an office to collect and confirm the information available publicly in social networks, within intelligence departments, emerged.

Intelligence after London 2011. The emergence of a new discipline of gathering intelligence – SOCMINT

The events that took place in 2011 in London were the starting point in terms of the emergence of social media intelligence. Nevertheless, this concept appears quite late in the terminology of secret services, if we are to take into account the massive promotion of phenomena on the social networks, such as the Twitter Revolution in Moldova in 2009 or the Arab Spring from 2010. But the scientific literature accepts the riots in London as the starting point in the analysis and use of what means social media intelligence or SOCMINT, because the events were a lesson learned for the Metropolitan Police, being the first to realize the need of collecting information also from this space. The Twitter Revolution in Moldova and the Arab Spring were seen as an important influence, as they were organized by extensive movements aimed at overthrowing the regimes in power, especially the communist ones, whose intelligence institutions had not considered or had only condemned and blamed social media involvement in the events that took place in 2009 and 2010, without taking into consideration the exploitation of all available information in social media.

Thus, overcome by the novelty and the speed with which information spread through social networks, departments specialized in gathering information from UK's Metropolitan Police were forced to take in their area of competence this virtual space too, assuming the mission to prevent and counteract threats from the online environment. Although at first many looked at that with skepticism, disregarding the new discipline of collecting intelligence, it began to play an important role amid the emergence of the informational era and knowledge society.

The head of London's Police Open Sources Department, Umut Ertugrul, declared that for OSINT he leads "*social media behaves like CCTV in terrestrial space*" (*Financial Review*), referring to the system of street surveillance cameras, available in England. According to Wired UK website, Scotland Yard would have recognized the existence of a team to monitor social networks and related posts that refer to political tensions. The team would be composed of 17 officers and would be named SOCMINT, having the mission to monitor Facebook, Twitter, YouTube and other social media services. This achieved 24 hours a day, 7 days a week continuity, stating also that this team of officers develop new means and methods to improve the intelligence activity. As a component unit of the Metropolitan Police, the team has jurisdiction in all districts of Great Britain and Wales (Wright, June 26, 2013).

Although through online media were circulated these information, tacitly recognized even by the OSINT director within London Police, Urmut Ertogral, there are still misunderstandings and uncertainties about what social media intelligence is or why it is necessary to approach SOCMINT among intelligence services.

Therefore, since the discipline is characterized by novelty, there still is no clear terminology of the phenomenon, but a series of works are starting, on the one hand, to tackle the issue directly, while on the other hand, other works study the related phenomenon. On this line, in the work Introducing Social Media Intelligence, considered the cornerstone of the approach SOCMINT, Sir David Omand outlines the new discipline as "*the existence of some capabilities through which authorities access data communication and access with warrant, when necessary, the communications content from the Internet, in this case social media*" (Sir Omand, Bartlett și Miller, 2012, p. 802). He also claims that the use of SOCMINT capabilities can contribute in a decisive way to ensuring public safety by identifying criminal activities, providing an early warning of the existence of tensions or public threat, or by creating a operational warnings when events evolve quickly (Sir Omand, Bartlett & Miller, 2012a, p. 9). Sir David Omand, together with his team, established what collecting intelligence from social networks means, which essentially can be summarized in gathering information available from the communication realized online via social media, also offering some examples of areas to ensure safety, be it national or international, as well as ways that SOCMINT can contribute directly to achieving this.

Other attempts to define what constitutes social media intelligence refer to "*collecting information from open sources by surveillance specialists in online socializing sites, chats, websites and Internet*" (*Use of Internet for Terrorist Purposes*, 2012, p. 68) or particularizes what SOCMINT means, as a subsequent area of collecting information from open sources, based on the idea that social media is an intelligence branch of OSINT, but has a specific action domain, in this case social networks (SOCMINT, October 26, 2012). Therefore it may be considered a new discipline of intelligence is emerging, still at an early stage of development and introduction to the work of the intelligence services. However, it is observed and materialized, even if for the moment, under the form of lessons learned, the opportunities that social media intelligence could provide with its implementation in the agenda of business information, opportunities that are not negligible, thanks to the contributions that they could make to ensure security.

Social Media Intelligence – opportunities for intelligence services

The lessons learned after the 2011 London riots lead to the necessity of introducing the concept of social media intelligence, as a new gathering intelligence discipline, among the classic ones like HUMINT or TECHINT, being at the same time a modern tool of harvesting intelligence, like CYBERINT. Research carried out regarding the London events and how the intelligence spread throughout the social media platforms revealed the fact that an analysis, realized in the spirit of the book and at a very specific moment in time, of the events released with the help of social media, would have been, in the end, a good early threat detection factor for Metropolitan Police, which, by using this tool, could have early combat and prevent the London riots and could prevent the swarm of conflict.

Therefore, taking into account all the things mentioned above, the perfect context for introducing SOCMINT on the working agenda of intelligence services was created, this new and young INT proving a series of opportunities of collecting primary data regarding a specific domain, such as riots or social unrest, and after that it would contribute to guaranteeing of the security climate within the capitalization of an analysis realized by the analysts of intelligence services.

Speaking about the opportunities brought out by using social media intelligence, it is said that the added value offered to the intelligence activity consists of the easing of the work of secret services through the simplification of collecting data about periods of time, locations of unfolding of events or individuals participating to this events. Apart from all of that mentioned above, there are some key concepts which make the object of studying the opportunities of social media intelligence.

Therefore, speaking about the opportunities brought out by the phenomenon of social media intelligence, the need to understand the utility of the *crowd sourcing* concept appears. James Surowiecki, a well-known journalist from *The New Yorker*, speaks about the intelligence of crowds and, at the same time, about gathering intelligence from crowds. His theories are associated with the theory of Gustave Le Bon regarding the idea of crowd. Subsequently, he argues that the idea that a few individuals who approach a specific domain or issue will bring out a better solution for solving it, rather than this problem would be solved by a person or two. In his book, *Wisdom of Crowds*, he explains the concept of crowd sourcing, emphasizing an essential aspect, that when we talk about intelligence of crowds, we don't speak only about brains put together, but decentralization. So, more individuals, among an extensive collectivity, will approach a specific issue and each person will have a key solution to it. Therefore, according to the theory, the idea that, in the end, a specific person will bring the best solution needed to solve the issue is promoted (Surowiecki, 2005). This phenomenon can be observed among the social media platforms. At the very beginning it was established that users disseminate content and information on a social media page. For instance, in the particular case of London riots, each Twitter user posted own beliefs regarding the events. In this context, we can speak about crowd sourcing from social media platforms, because the Metropolitan Police had the chance to analyze all these tweets (gathering intelligence), to check them for validation (verification), to analyze in order to establish action directions (analysis) and, in the end, to choose the best way of action, all of the above being based on intelligence gathered from social media platforms, in order to prevent or counter the riots. By these means, the utility and the necessity of crowd sourcing activity can be proven, all these being pictured on the key core of intelligence activity, the intelligence cycle.

Another dimension of this phenomenon, in term of opportunity of SOCMINT for intelligence service, is generated by Sir David Omand, who is the promoter of the idea that speaking about crowd sourcing, from the institutional point of view, we can speak about a better information flow between citizens and governmental institutions, especially when there are critical situations. He starts his research from the idea that persons who assist at the birth of a specific event can become journalists for a minute, having the chance to post on social media intelligence from the field, intelligence which can be subsequently used by intelligence officers. Through the facilities offered by social media, but especially throughout the possibility to disseminate multimedia content, these journalists can post photos or movies from the field, which can be used by law enforcement institutions in order to start new operations. By connecting the concept of crowd sourcing with the concept of wisdom of crowds, regarding the intelligence services` activity, a platform, was established called Ushahidi, where individuals can post intelligence, no matter of its nature, such as information regarding the Haiti earthquake or traffic jams from Washington (Sir Omand, Bartlett și Miller, 2012, p. 805). Thus, with small steps, the basic levels of a new technology which can provide citizens with the chance to contribute actively to the security climate are established.

Another opportunity of the emerging social media may consist in the research and the insight of social network analysis. The study of the social media platforms could help the secret services understand certain emerging phenomena within WEB 2.0. This could reveal some essential facts, like violence indicators, Islamic terrorists' ways of promoting self-radicalization or limits and indicators of criminality brought by the social networks. Thus, this thing can contribute to the understanding of the possibilities of forming and changing certain ideas and for investigating the link between social media and technology, between an off-line status and an on-line (Sir Omand, Bartlett și Miller, 2012, p. 805) one, for having a guarantee of a built-in knowledge of both the phenomena and their initiators.

Besides the above mentioned things, the opportunities provided by SOCMINT also include the concept of real-time operational intelligence of the activities developed in the virtual space of the social networks. The analysis of Twitter statistics revealed that there are postings both before and after the manifestation of a phenomenon. Therefore, the evaluation of the social media platform traffic, could facilitate the identification of emerging phenomena, a process carried out much easier as compared to the application of the traditional investigative techniques for the same purpose.

For instance, if the geolocation of the events promoted in the social media could be determined, then the intelligence analysts could obtain evolution maps for the possible new physical locations of a protest, revolt and, why not, of a criminal act (Sir Omand, Bartlett și Miller, 2012, p. 805).

Regarding information gathering via the activities developed and promoted within the social networks, one could speak about knowing the people and groups developing such activities. Terrorist or extremist groups frequently create pages on Facebook or Twitter in order to promote their ideology, their messages, and their own values. Thus, intelligence officers are given insight into these groups, achieving a better understanding of their mentality and action modalities. In this sense, one could study the level of social discontent existing within the group, of the state of tension of its members or of the main motives that animate the users' activity.

SOCMINT can be also used by intelligence services to identify criminal, extremist or terrorist intentions through large scale monitoring operations of the social networks run by specialized technical officers who have the possibility to survey the activity of the groups and people known as developing actions which could pose a threat to national security (Sir Omand, Bartlett și Miller, 2012, p. 806).

However, it is not only the terrorist or extremist groups that organize themselves through social media in order to enlist new members. After the emerging social networks phenomenon, intelligence services have also begun a vigorous campaign of recruitment through this space. These campaigns have two directions.

On the one hand, one could speak about promoting security institutions and their transparency together with their call for personnel, following the model of private companies which by help of marketing campaigns promote their image and look for personnel. On the other hand, there is a particular aspect regarding the intelligence service, that is, recruiting new intelligence agents and appealing to the collaboration of resourceful people from the medium of interest. It follows then that, by combining a classical INT- HUMINT with a modern INT, that is SOCMINT, the intelligence platform is prepared to ensure security.

In this sense, for instance, the British Intelligence Services (MI6 and SIS) used a Facebook application to recruit their personnel, to fill out questionnaires and to attract people coming from different social media.

CIA has also created a Facebook page for recruitment only, Mark Zuckerberg's network being accused by different media that it would represent a means of the Central Intelligence Agency's activity due to the fact that the American service has invested large sums of money in the technology of social media surveillance. In this context, "the recruiting mode as well as the agency's coordination method and specific means of the intelligence activity observe the same conspiratorial rules, having the great advantage of a better conspiracy and a larger operational level"(Ciupercă, Ciupercă, Niță & Stoica, 2010, pp. 124-125) as all is done remotely, without exposing the intelligence officers, as they operate behind a computer" (Ciupercă, Ciupercă, Niță, Stoica, 2010, pp. 126-127). Under these circumstances, the intelligence services can operate in social media, under conspiratorial profiles, simulating real life cover either to establish connections with future agents or to get in the relational background of those targeted who, in their turn, due the anonymous character of the social networks could be more open to cooperating with intelligence services. At the same time, through these platforms, the intelligence officers could verify persons' alibi by comparing the stories they provide "to their activity within the social networks"(Ciupercă, Ciupercă, Niță, Stoica, 2010, pp. 126-127).

However, if a future recruitment of possible sources or agents is commendable, this time in a real, tangible space, when the people in question are known as being active on social networks, the intelligence officers can collect primary data on them, by following some standard criteria, available, for instance on Facebook, thus obtaining the agent's or the source's profiling.

In this sense, a first step in the learning process can be the profile picture or pictures as well as other pictures posted on the user's page. If the intelligence officer has only the name of the person (or his username) listed in a relational circle of suspects, without having the possibility, at that given moment, of collecting other significant data and if other information previously recommended him for selection and recruiting, then the said officer can proceed with the verification of this person on Facebook.

If one or several profiles corresponding to the name obtained are found, the officer can identify the respective person by comparing data recorded in the population register with those found on Facebook, as to confirm the correspondence between the real name or the username and the Facebook profile. In this sense, one can compare the date of birth recorded in the population register with the date of birth of the profile, thus facilitating the above mentioned correspondence and the full identification of the checked person. Consequently, the intelligence officer can access the user's profile picture or pictures which results in identifying and knowing that person. Besides the physical aspects, the officer can gather information through posted pictures, about the user's relational circle, having, in this way, the possibility of watching both the way in which this person spends his leisure time and the people surrounding him; through this possibility he can identify the hobbies and even the vulnerabilities that he may use later. All this helps the officer in becoming acquainted with that person before the real meeting, as he has learned some details that he can use during their discussions concerning recruiting.

A further step in the fulfillment of the person's profile meant to be recruited, made by the intelligence officer is to survey the personal data posted by the checked person on his personal page. In this respect, another helpful thing for the intelligence officer who has to determine that person's profile, is the exposure of personal data, data that some users choose to make public in their account.

These are data concerning date and place of birth, education, coursework in progress, employment, marital status, residence, relatives and other contact data (sometimes even email or phone number). There are also two subsections within this section, which allow the user to include an additional description about himself and to add favorite quotes from various writers. The above mentioned data help the intelligence officer to establish those significant details regarding the education level, family, income and also to determine the psychosocial and behavioral traits of the person involved, which following an attentive analysis, he can use to establish a psychological profile of that person.

The friends and the connections the user made on his personal page can constitute the next essential aspect which the intelligence officer is to take into account in order to establish the checked person's profile. Thus, the officer who builds the profiling through the analysis of the user's friendship relationships and of his other contacts from the social media, completes his knowledge on the relational circle of the person chosen for recruitment.

A careful observation of the people added on the user's account and the analysis of the close relationship they have with certain people can lead to understanding of a particular relational background and to establishing of its specific features by identifying the social status of the person, the social milieu he frequents as well as his most comfortable surroundings. Therefore, important data can be obtained concerning the motivation for recruitment or the creation of a favorable recruitment context.

Check-in option, together with location services offer a great opportunity to the person who analyzes the chosen user's profile. He can observe in real time where the chosen person is, at a given moment, if this person utilizes check-in function while being in a certain place. In this way, the officer knows precisely where the person is situated, following GPS coordinates given on Facebook and also the names of public or private locations available in check-in function. Consequently, if the person posts something, the approximate posting location can be determined so that the officer in charge could check the presence of the said person in a certain neighborhood, district, and region.

In this sense, the intelligence officers can appeal to this profiling method by means of social media, to obtain, through the analysis of a few key elements of the Facebook network, primary data concerning the future candidates for recruitment, which when corroborated and verified by comparing them with other information collected from different sources, can give an overall picture on the recruitment of the new information sources, on their quality as well as on the psychological features which led to the start of the recruiting process.

If, at the information operations level of the intelligence activity one could speak about obtaining a profile based on primary data, gathered via social networks, about the candidates for recruitment, then, within the technical side of this activity – as it was stated that even in this area the information collecting activity develops observing the same rules, means, methods, and principles –, social media is backed up by opportunities such as social network analysis software, easy- to -use by the intelligence services analysts.

In this context, a series of programs have been created whose utility in social network analysis is given by the easy way they produce graphical representations as a cobweb diagram for a better comprehension of the 2.0 network representation in the tangible reality.

Starting from the idea that, succinctly, a social network stands for a finite set or finite sets of actors connecting to each other, it follows that social network analysis implies detecting and interpreting the social patterns of the characteristics that bring actors together, all of these being represented graphically by means of the already mentioned programs (Everton, 2013, p. 9).

Such an example of a program is UCINET developed by Linton Freeman when he was teaching in the University of California. The name of the program, Irvine, was derived from this place; this program was afterwards upgraded several times. This is one of the best known social network analysis software and also most used as it incorporates a series of measuring tools for data provided by social channels as well as other data management tools. All these contribute to estimating measurements of the network topography, giving information on the central actor of the network, identifying subgroups and estimating the measurement values of the structural equivalence of the considered platform.

Moreover, UCINET provides several tools for data subset selection from the network and for data import and export in any format; all these features make of UCINET a powerful program used in social network analysis.

Conclusions

Accordingly, it may be concluded that the use of software intelligence based on a 2.0 dimension, through social media analysis, creates numerous opportunities that could be utilized by intelligence officers to obtain additional information for an investigation topic and sometimes to obtain new aspects on the information which could not be observed by the field officers. In this context, if the implementation of INTs 2.0 is supported, their utilization could offer the missing pieces of a puzzle which direct the activity the intelligence services (Everton, 2013, p. 50).

However, one should take into account the simple fact that those who use social media for purposes that do not serve the values and national interests, could become aware of these opportunities and that they could become the first beneficiaries of them; therefore social networks and the internet remain an area to explore, a demilitarized zone where both groups wishing to affect the security environment and the intelligence services are acting and fighting for digital supremacy. The question arising from this situation can be formulated then as: how much risk is each one willing to take to conquer the digital sphere?

Will the intelligence services be ready to carry out a new research and knowledge activity in order to understand the new phenomena or will these groups protect their leaders, sympathizers, methods so well that the international intelligence community would fail to collect the necessary data? While taking into consideration the above mentioned opportunities and the emerging activities undertaken by groups that can produce threats to national, regional and international security and affect the values and the interests of the states and of non-state actors as well as the continual fight between the intelligence community structures and these groups, one cannot and must not lose sight of the fact that there are limits for the data collecting activity via social media intelligence.

References:

1. Ciupercă, Ella, Ciupercă, C., Niță, C, Stoica, M., (2010), *Rolul rețelelor de socializare pe internet în modelarea comportamentelor*, București: Editura ANI.
2. Everton, Sean, (2013), *Disrupting Dark Networks*, Cambridge University Press.
3. *Financial Review*, available on www.afr.com/p/technology/google_glass_and_social_media_to_R5en8jIWOeVUjasiJqsaIL.
4. *How riot rumours spread on Twitter*, (December 7, 2011), în *The Guardian* available on www.theguardian.com/uk/interactive/2011/dec/07/london-riots-twitter.
5. Le Bon, Gustave, (2012), *Psihologia mulțimilor,* București, Editura Antet.
6. Lesidrenska, Rada, Bancheva, Vessela, (2012), *Adaptation of Intelligence and Security Services to Contemporary Challenges* în Proceedings of the XVIIIth International Conference – Intelligence in the Knowledge Society.
7. Lewis, Paul, (August 7, 2011), *Tottenham riots: a peaceful protest, then suddenly all hell broke loose*, în *The Guardian,* available on www.theguardian.com/uk/2011/aug/07/tottenham-riots-peaceful-protest.

8. Maior, George Cristian, *Mesajul directorului Serviciului Român de Informații* în *SRI în era informațională, Viziunea strategică 2011-2015*.
9. *Mark Duggan inquest and reaction*, BBC News accesibil pe www.bbc.com/news/uk-england-london-25648913.
10. *Pagina oficială de facebook R.I.P. Mark Duggan* available on www.facebook.com/pages/RIP-Mark-Duggan/200659976657547.
11. Philips, Richard, Frost, Diane, Singleton, Alex, (2012), *Researching the riots* în the Geographical Journal.
12. Sir Omand, David, Bartlett, Jamie, Miller, Carl, (2012), *Introducing Social Media Intelligence,* în *Intelligence and National Security*, Vol. 27, Nr. 6.
13. Sir Omand, David, Bartlett, Jamie, Miller, Carl, (2012a), *A Balance between Security and Privacy Online Must Be Struck*, în Demos.
14. Social Media Intelligence (SOCMINT), (October 31, 2012), Same Song, New Melody?, available on www.osintblog.org/2012/10/31/social-media-intelligence-socmint-same-song-new-melody.
15. Surowiecki, James, (2005), *The Wisdom of Crowds*, Anchor Books.
16. *Use of Internet for Terrorist Purposes*, (2012), Oficiul Națiunilor Unite pentru Droguri și Criminalitate.
17. Wright, Paul, (June 26, 2013), Meet Prism's little brother: Socmint, available on www.wired.co.uk/news/archive/2013-06/26/socmint.

HISTORY AND MEMORY IN INTELLIGENCE

REASONS FOR DEFECTION. HISTORICAL CASES ANALYZED THROUGH CONTEMPORARY MODELS

Ioan CodruŢ Lucinescu*
Valentin Stoian[1]

Abstract

The article aims at harnessing the analytical power of theoretical models employed in studying defection in favor of the enemy and use them to study Romanian historical sources originating during the First World War. These models have been developed in the United States during the 1950s and 60s and are used by this article to study a very different case. The article's main research question is "Can models explaining reasons for defection developed in the US during the Cold War be applied on behaviors detected in Romania at the beginning of the XX century?" The article answers this question in the affirmative, showing how reasons for defection are, many times, similar despite large differences in time and space.

The article's first section relies on an exhaustive review of several theoretical models, especially MICE. Further empirical studies have refined this simplification of motivations, uncovering new potential reasons for betrayal such as the existence of "divided loyalties" or of disgruntlement against one's own organization. These represent the analytical blueprint which is later applied on Romanian documents dating from World War I.

The second part of the article employs an analytical approach to uncover reasons for defection in Romania and its vicinity. It presents both cases of ethnic Romanians who were Austro-Hungarian citizens and defected in favor of Romania, as well as intelligence successes by the Austro-Hungarian enemy in Romania of that time. The article concludes that the first cases are mainly motivated by "divided loyalties" while the second was mostly caused by money and ideological reasons.

Keywords: defection, motivation, ideology, loyalty.

Introduction

Both fictional literature and popular action movies, many times simplified versions of complex realities, employ the image of the traitor as an even more radical form of evil than that of the main antagonist. Treason or

* "Mihai Viteazul" National Intelligence Academy.

[1] "Mihai Viteazul" National Intelligence Academy.

defection is, many times, portrayed as the action of a weak person, tempted by underserved benefits or acting out of unjustified envy, delaying, but never stopping the success of the main protagonist.

Reasons for defection in the world of real espionage are, many times, more complex. Especially in situations of war or of heightened ideological confrontation, defection represents a serious risk to one's own person and the reasons that individuals have to accept these risks are diverse. Moreover, one has to mention that, many times, those that accept to work against their own state for a foreign power are never caught and their reasons for doing that are never known. In many other situations, although those that commit such actions are caught, documents that reveal their motivations (either documents generated by the intelligence service that recruited them, or transcripts of after-the-fact interrogation) remain classified for a long period of time. Thus, their reasons for action can only be analyzed long after the fact.

The present article employs an innovative approach in the field of intelligence studies, using a theoretical model developed by American specialists during and after the Cold War, on Romanian historical sources relating to the First World War. The article aims to answer the following research question: "Are analysis models developed in the US during the Cold War useful in analyzing Romanian historical sources from the early XX century?" The article answers the question in the affirmative, showing that these models can accurately describe the main reasons for defection of both ethnic Romanians from the Austro-Hungarian Empire, which did so out of "divided loyalties", and of Romanian citizens working for the Austro-Hungarian enemy for financial reasons. Of course, the two situations do not exclude each other, and both are encountered in all cases. However, certain patterns prevail on each side of the barricade. The differences are determined by the different political and military situations of the two combatants: Austria-Hungary ruled over a vast territory where ethnic Romanians were the majority and had undertaken, in the recent past, a violent cultural assimilation policy of its Romanian subjects, leading to alienation and frustration. On the other hand, the Dualist Empire could mobilize superior financial resources and exercise considerable cultural attraction.

The article's first section will present theoretical models of defection in favor of an enemy intelligence service, models coming out of the research of concrete cases in the United States of America. These emerged in the context of the unprecedented development of Soviet espionage in the US resulting in the interviewing of a large number of American citizens which had worked for the Soviets. The main model discussed is MICE (Money-Ideology-Compromise-Ego), which several intelligence studies mention, in both theoretical and empirical papers. This was modified several times, sometimes radical changes being advocated.

The second section applies these theoretical models on Romanian historical sources during the First World War, analyzing both the reasons for defection of ethnic Romanians from the Austro-Hungarian Empire, as well as that of Romanians working in favor of the Central Powers. The section concludes that the first phenomenon was far more widespread, and it mostly involved persons of an average social status, attracted by the idea of serving a state that they identified with more, while the second was mostly financially and ideologically motivated, and mostly involved political-military elites.

Beyond the scientific conclusions, one can also state that human motivations are universal, as similar actions were similarly motivated in different times and political-military contexts. Thus, this study allows one to express views on the usefulness of both theoretical models, as well as on universal laws of human motivation.

Literature review

The literature analyzing the motivations of people who defected in favor of the enemy is wholly reliant on American cases which occurred during and after the Cold War. Considering the large number of espionage cases occurring in the US, but also the government's desire to elaborate a profile of the spy, the most important empirical research on convicted spies occurred in this country. To some extent, the literature on the motivations of US citizens convicted of espionage against their own country is contextually dependent on the political situation in the period in which the convicted people acted. On the other hand, certain other kinds of motivations can be extended to other historical periods and political situations. What remains constant, during all times, is that a person who accepts to become a human source for an enemy intelligence service on the territory of the state whose citizen he is, exposes himself to extreme risks, as the death penalty or life imprisonment are common especially during wartime. Thus, although the political situation differs, and some specific situations are not included in the American literature on US citizens committing espionage during the Cold War, this literature can provide a guide to basic motivational categories for defection.

The literature on intelligence studies employs the MICE model (Money-Ideology-Compromise/Coercion-Ego) to describe possible motivations of a person who accepts to become a human source for an enemy intelligence service. According to some authors, this general model was presented, for the first time, to the public by Stanislav Levchenko, a KGB major, who defected to the West in October 1979 (Lowenthal, 2011, p. 150;

Charney and Irvin, 2014). According to this model, four motivations determine a person to become a spy against one's country or organization.

Money is proposed as the first reason in this model. It is one of the most simple and easy to understand motivations. A large part of US defectors, but also of those used by the CIA to spy on the Soviet Union, were financially rewarded. One of the best known cases is that of Aldrich Ames, who was uncovered due to his extravagant expenses. A specific form of this motivation is described by Sebastian Michalak, a Polish researcher who quotes an internal study of the Security Service of the Polish Ministry of Interior from 1980. This study mentions that about half of Polish citizens who spied in favor of Western Countries between 1957 and 1970 did it directly for money, while another quarter were motivated by a desire to be supported in their attempt to emigrate to the West (Michalak, 2011).

Ideology refers to a set of beliefs about what is correct in the world, either in general, or in what regards a country's policy in a certain field. Generally, according to the literature, ideologically motivated espionage was a characteristic of the first period of the Cold War, considerably decreasing during the second part of the conflict, but coming back, to some extent, after the Cold War. The drop suffered in the second period of the Cold War was determined by the revelations about the Soviet policies, which reduced the attractiveness of the communist ideology. The best known cases of ideological spies are the "Cambridge Five" group, out of which Kim Philby is the best known, and Ana Belen Montez. These spied against the UK and the US respectively due to their belief that these governments were mistaken in their ideological orientation (Burkett, 2013). Philby spied in favor of the USSR, while Montez did the same in favor of Cuba. Moreover, with the collapse of the Soviet Union and the rise of a threat from radical Islam, a series of American citizens began to defect in favor of al-Qaida, convinced of the need for global jihad (Herbig, 2008).

Compromise/Coercion includes the blackmail of people or their coercion through other means (ex. threats against one's family) to determine them to commit espionage. Fictional literature refers to men seduced by female agents of foreign intelligence services or of gay men blackmailed because of their sexual orientation (Charney and Irvin, 2014).

Ego involves the defector's belief that he is superior to those around him due to his activity or to the desire of thrills to escape the daily routine. Those having these reasons for betrayal image that their activity offers the possibility of an adventurous life, making them believe they are better than others (Burkett, 2013, pp 7-9).

Other theoretical approaches come to complete or modify the MICE model, recommending new factors that explain reasons for defection of people involved in espionage activities. Stan Taylor and Daniel Snow (1997) recommend the replacement of the last two reasons (Compromise/Ego) with the "Ingratiation" and "Disgruntlement". The first refers to the desire of the defector to please someone, especially a friend/lover, while the second describes a situation where the potential defector is dissatisfied by the way the organization that he is part of treats him and decides to take revenge. The best example of such a situation is an employee who believes that he would have deserved to be promoted, but was not or that he was unjustly punished (Taylor and Snow, 1997, pp. 101-125). Another possible factor that determines espionage in favor of another country is, according to the PERSEREC report (see below) the existence of "divided loyalties", that is, a situation where a person, either due to cultural or to family connections, feels closer to another country than that whose citizen he or she is (Herbig, 2008).

A radical change of the MICE framework or of its different versions was suggested by Randy Burkett, a CIA representative to the US Navy post-graduate school. He recommends the replacement of the MICE acronym with RASCLS (Reciprocation-Authority-Scarcity-Commitment and Consistency-Liking-Social Proof). This model is constructed on the universal principles of human action suggested by Italian psychologist Cialdini. These are, according to Cialdini's theory, Reciprocation, Authority, Scarcity of Resources, Commitment and Consistency, Liking and Social Proof. According to Burkett, reciprocity means the recruiter's availability to help a potential source with a favor or to fulfill a need before requesting anything. According to psychological theories, people feel compelled to repay a favor that was done to them. Authority presupposed the adoption of a posture suggesting that the recruiting officer is part of an important organization which can considerably influence the course of events. The third term, translated as limited resources, presupposes that the recruiting officer tell his source that what he can provide is urgent and important in the given situation, and, thus, to generate, immediate action. According to Burkett, it is necessary that an intelligence officer prove that he is fully committed to the relationship and does not change his behavior, while requesting the same from his source (commitment and consistency). Then next term presupposes that the source be flattered, so that a pleasant human relation ensues between the officer and his source, while the last (social proof) requires the suggestion that the agent is not alone, that other agents exist and that defection is desirable behavior also for other people (Burkett, 2013).

Three major sources of empirical studies have been documented by this article: academic articles, the Slammer project report and the reports of the PERSEREC project. These have researched the motivations of individuals involved in espionage activities against one's own country. Unfortunately, all these studies were made in the US and exclusively refer to citizens that spied against this country. Motivations for defection in other contexts can be analyzed only through the secondary analysis of academic articles discussing espionage cases, but not expressly focusing on motivations.

In the above mentioned article, Stan A. Taylor and Daniel Snow analyze the cases of 139 Americans officially charged with treason in the United States and employ a four-factor motivational schema: Money-Ideology-Ingratiation-Disgruntlement. The two authors analyze only the period 1940-1990 (the Cold War), and employ open sources to establish motivation for each case. The two authors attribute motivation directly, without access to detailed interviews with those accused of espionage. The article concludes that the financial and ideological motivations are similarly important between 1940 and 1970 (especially during the first two decades of the Cold War), while during 1970-1990, the importance of financial motivation increases significantly, while the other factors decline. According to the authors, the very low pay of military personnel in lower positions (enlisted personnel, non-commission officers), generated significant temptations and favored espionage. Only 23,7% of the total spies committed their crimes for ideological reasons, a much lower percentage during the 70s and 90s, especially after the revelations of the crimes of the Soviet Union and the crushing of the Hungarian (1956) and Czechoslovak (1968) uprisings (Taylor and Snow, 2007).

Psychologist Leroy Stone (1992) undertook empirical studies on the motivations of those who committed espionage against the US. He built a database of 186 persons accused of espionage, employing 59 motivational variables. The coding for the variables was done by consulting open sources for each case. As in the study performed by Taylor and Snow, Stone imputed motivations by himself, relying on the use of open sources. By employing the method of Principal Component Analysis (a statistical method implying the grouping of primary variables in new variables generated automatically), Stone concluded that a visible difference exists between financially and ideologically motivated defectors. Thus, those that betray for money, do not have ideological motivations and vice versa. Moreover, the author could not detect any relationship between other motivations for defection, such as the state of one's career, each of these being self-standing motivations (Stone, 1992).

One of the most important sources of studying condemned spies in the United States is the PERSEREC project of the Defense Personnel and Security Research Center. This center was founded by the United States Department of Defense, after the scandal caused by the defection of John Anthony Walker (an US Navy NCO, who sold classified documents to the Soviets and was arrested in 1985). This research center was founded to fulfill the recommendations of the Stilwell commission, which evaluated the weaknesses of the system of granting access to classified documents in the US. The PERSEREC project holds the largest database of persons convicted for espionage against the United States, generating, up to date, three reports on their motivations. The most relevant report for this article is the last, which included espionage activities between 1947 and 2007. Again, one has to mention that motivations for espionage were imputed by researchers on the basis of consulting open sources, without directly talking to those condemned for espionage. The PERSEREC reports use a motivation schema divided between: money – divided loyalties – disgruntlement – ingratiation – coercion – thrills – recognition/ego. Unlike other studies, this report includes the possibility that a spy is motivated by different factors, presenting data on the prevalence of more important reasons when several exist (Herbig, 2008).

Similarly to the study by Stan and Taylor, the third PERSEREC report observes the increase of the financial motivation in the second period of the Cold War, followed by its decrease in the period after the conflict's conclusion. If, in the first part of the Cold War (1947-1979), spies that had money as the sole motivation represented 47%, this increases to 74% during 1980-1989, and dramatically decreases to only 7% between 1989 and 2007. Moreover, the percentage of spies motivated primordially, but not exclusively, by money varies between 43% and 60%, to decrease to only 39% after 1989. Alternatively, the existence of divided loyalties as a sole motivation falls from 16% between 1947 and 1979 to 11% between 1980 and 1989, a jump being later observed to 57% after 1990. A similar evolution is seen by divided loyalties as a primary rather than a sole factor. Disgruntlement reaches 22% for the period 1989-2007, after its importance had been diminishing during the previous period. Other possible motivations are less relevant, as the number of cases that they cover is much smaller. One of the report's conclusions is that espionage against the US after 1989 is heavily influenced by the globalization process, many defectors being naturalized American (foreign-born citizens), who keep cultural connections with their (or their parents') country of origin (Herbig, 2008).

Another source of information on the motivation of those condemned for espionage against the US is the Slammer report (thus entitled as the research was undertaken in maximum security prisons where the condemned were locked up – therefore the term "slammer"). This was carried out under the auspices of the CIA at the end of the 1980s and in the beginning of the 1990s, the report being finalized in April 1990, but partially declassified only 16 years later (Stein, 2010). Unlike previous studies, the Slammer project report relied on the detailed interviewing of 30 people sentenced for treason, taking advantage of the presence of a specialized psychologist and a counterintelligence officer. Moreover, family members and persons close to the defectors were interviewed, so that their real motivation can be studied. Thus, the project could identify the motivation of sentenced spies more directly, rather than through open sources. The synthetic information presented publicly shows a profile of the traitor as mostly motivated by disgruntlement against the way that the organization he is part of is treating him, as he believes that he would have deserved more, for example a promotion or a better material situation (Project Slammer Interim Report, 1996). Moreover, the traitor believes he is better than other colleagues and that his organization does not accept that. Moreover, those sentenced for espionage believe that they are superior to the security procedures established by the organization and their success in working undetected for a specific period reinforces that. One way that spies use to detach themselves from the results of their own behavior is the perception that their actions do no harm to concrete individuals, a potential change in the " global balance of powers" being perceived as an extremely abstract possibility (Project Slammer Interim Report, 1996). Psychologist William Pollack, a US psychologist, issued the hypothesis that the money received by the convicted spies are meant to validate one's own ego, which the organization wounded (Pertman, 2001).

Unlike static models presented above, Terrence Thompson, a former CIA psychologist (the head of the polygraph testing division), who interviewed a part of those condemned for treason, elaborated a dynamic evolution model of the person committing espionage. According to Thompson, the decision of beginning espionage activities is taken at the intersection between "opportunities, a life-crisis, a negative character trait, triggered by a particular event". Thompson believes that the access to classified information represents an opportunity to commit espionage. In most cases, life crisis is created by the absence of enough income, by a sudden move decided by superiors, or by the reevaluation of life which the mid-life crisis causes (in the case of Robert Hanssen, he could not afford to take his children to catholic school, as he perceived his religion requests). Weak character traits are, according to Thompson, the predisposition to crime or to a life of luxury, which was present, for example, in Aldrich Ames. To reduce the negative character of one's own actions, most spies believe that their actions are not evil, but that they are doing a good deed. For example, Earl Pitts said that he wanted to get revenge against the FBI, but is not really betraying his country. Finally, the triggering event came due to situations such as financial or marital problems (Thompson, 2014).

Other cases revealed by specialized literature did not focus exclusively on motivation, as they were analyzed in the context of studies on intelligence activity in certain states and in certain periods of time. An article on MI5 operations against the Irish Provisional Army presents the case of an agent called "Observer B", who offered information to British intelligence on the activity of the terrorist organization, but also of rival militant groups (belonging to protestant loyalists in Northern Ireland). According to the case officer, "Observer B", could be considered an ideologically motivated agent, as his main motivation was the desire to "combat extremism and violence, regardless of their source". Therefore, in a confidential report consulted by the author of the article, "Observer B" is described as "having a desire for peace", but also as a powerful "anti-Republican, intensely loyal to the United Kingdom, but deeply opposed to the use of force by the protestant community to impose its will on the Ulster Government and the Roman-catholic minority" (Charters, 2013).

A study on KGB operations that took place in Israel during the Cold War revealed that the main motivation of those who chose to work for the Soviet intelligence service was money. One of the spies, Israel Bar, became a target for a counter-intelligence operation because of the luxury lifestyle he led, which contrasted significantly with the relative scarcity of Israel in the 1950s. Another example was that of Levi Levi, who worked for Polish intelligence inside the Israeli counter-intelligence service (Shabak or Shin Bet), becoming a suspect due to a golden chain he wore. The only case of ideological motivation presented in the article was Zeev Avni, who worked for the KGB due to his communist beliefs. The article concludes that the soviet service offered large sums of money to its agents in Israel, and this constituted the main motivation for espionage activities (Shpiro, 2011).

Other sources to establish reasons for defection can be memoirs, such as those written by Henry Crumpton, a former CIA officer. These can represent a source for assessing the motivations of those who worked in favor and not against the United States. Crumpton used the MICE system to describe the motivation of his sources. In his recollection, he presents the case of financially motivated sources, who were led to commit espionage by the low pay they received. Further, Crumpton discusses the situation of an African tribal leader willing to help the US because he believed tribal organization was obsolete and conducive to violence. Then, he focuses on the case of an encryption officer in an Eastern Bloc embassy, compromised after losing a large sum of money or that of a small-time civil servant who was disgruntled by being ignored by all in his organization (Crumpton, 2013).

Espionage and betrayal in Romania and its vicinity, at the beginning of the XX century

Although the theoretical models presented above have been mostly elaborated relying on the experience of the Cold War, the attempt to employ them to analyze events occurring in Romania and its vicinity at the beginning of the XX century will confirm that reasons for defection can be studied according to universal patterns.

Since 1915, when it became obvious that Romania would join the Entente, and that the Romanian army would begin its offensive in Transylvania, national intelligence structures aimed at ensuring a continuous and diversified information flow on Austro-Hungarian military capabilities to the Bucharest decision-makers.

In addition to providing counter-intelligence support for the Romanian Army, Romanian intelligence structures organized, during the two years when Romania was a neutral party (1914-1916), complex intelligence actions in Transylvania.

To this end, Romanian intelligence especially aimed to recruit persons whose employment was of such a nature that they could easily travel without arising suspicion, especially during wartime, when the movement of people and goods is heavily restricted in all belligerent states.

The main reason for defection by Austrian subjects of Romanian ethnicity was the existence of "divided loyalties". Many of them felt closer to Romania, which they perceived as "their country" and, many times, felt a desire to contribute to the potential union of Transylvania and Romania. One cannot deny that some of these collaborators also received material compensation, but it was not this that motivated them to take such a perilous course of action (in case they were discovered, the sentence was generally death by shooting or hanging). Moreover, the employees of Romanian intelligence structures, both of those belonging to the Ministry of Interior and to the Ministry of Defense, aimed to predominantly recruit Romanians who had already shown signs of sympathy for Romania. Most human sources were recruited from among intellectuals – doctors, pharmacists, lawyers, professors, engineers, primary school teachers or priests or state employees such as forestry employees, postmen, railway workers or salesmen (Brestoiu and Bobocescu, 1979, p. 105).

Documents elaborated by the agents of State Security (the Ministry of Interior's intelligence structure), point out to the presence of the consciousness of belonging to Romania among their collaborators. In a Note elaborated on the 23rd December 1914 addressed to the leadership of the

State Security, one of its agents describes the extent of the help that could be provided by Greco-catholic (uniate) priest of Iablanița, George Tătucu. According to the note, he is described as "He is a worthy man, honest, untainted, maybe the most trustworthy Romanian priest in Caransebeș. Worthy of all the Romanian State's trust" (ANIC, DPSG, 592/1914, f. 2).

The same agent points to the orthodox priest Iulius Musta, of Glimboca (Banat), who could offer important services given his good knowledge of trans-Carpathian travel routes which would be vital to Romanian troops about to cross the mountains. As he was in Bucharest on business in December 1914, the State Security agent requested permission to recruit him immediately so that he could provide intelligence as soon as he returned to the Banat. Moreover, given the good material condition of the two priests, it was estimated they would not require any form of compensation from the Romanian state for their secret activity (ANIC, DPSG, 592/1914, p. 3).

In addition to numerous and well-motivated civilians, we also encounter imperial army officers who betrayed their country out of patriotism and worked in favor of Romania. Strategic intelligence was obtained, according to what Marshall Alexandru Averescu states, from an ethnically Romanian hussar, who, in 1916, deserted the imperial army and crossed the mountains. In Bucharest, he pointed out to the Romanian General Staff that the Central Powers Campaign plan against Romania foresaw the occupation of Oltenia as its main objective, to be reached from the very beginning of hostilities.

"I came to believe this information – pointed out Marshall Averescu in his notes – as it was evidence of an intelligent plan and, when the enemy undertook efforts and concentrated 3½ divisions – I supposed that the goal was to isolate Oltenia through the occupation of Pitești" (Averescu, p. 365).

By studying archival documents, one can observe the complexity of intelligence activity carried out in the Austro-Hungarian Empire during the two years of neutrality (1914-1916). It is estimated that approximatively 1.000 persons (Ștefănescu, 2009, p. 41) – Romanians, but also other individuals belonging to other nationalities who lived in Ardeal – were agents of the Romanian Army, State Security or the Gendarmerie. Obviously, they were considered "traitors" by Austro-Hungarian authorities, and were severely punished if discovered.

Eugen Cristescu, the head of the Special Intelligence Service (1940-1944) wrote about this topic: "Through offensive intelligence action, State Security and the General Staff succeeded in obtaining intelligence on Austro-Hungarian military movements, employing especially Transylvanian

Romanians, who were used as informers and who, at the end of the War, were employed as superior civil servants in the Security Service of Great Romania" (*Din Memoriile lui Eugen Cristescu*, 1968, pp. 14-15).

From General Maximilian Ronge, the head of the intelligence service of the Austro-Hungarian Empire during 1914-1918, we can find out that a significant number of cases were discovered by the imperial counter-intelligence services during the two years of neutrality; over 100 cases of "treason" by civilian and military citizens of the Habsburg monarchy in favor of Romania were discovered (ANIC – MR. MSM, 119, pp. 181-182).

On the other hand, the intelligence services of the Central Powers also recorded notable successes in recruiting high military and political officials in the Old Kingdom, especially during the period of Romanian neutrality. The main reason for this betrayal was a financial one. We can recall the case of General Vasile Zottu, the head of the Romanian General Staff during 1914-1916. The general's destiny is tragic, as he committed suicide on the 12th of November 1916 after Romanian State Security agents stole, on the 16th of August 1916, a briefcase out of the car that the German ambassador, baron von dem Busche, was using to depart Bucharest. The briefcase contained an "explosive" document: the 200 page list of the "parties, officers, politicians, journalists and real-estate agents who allowed themselves to be corrupted" (Neagu, Marinescu and Georgescu, 1977, pp. 86-87).

In order to show the extent of the corruption, we can point to the discovery of a letter through which the German intelligence center in Sofia communicated to the Reich legation in Bucharest that the sum of 25 000 gold-marks had been sent to support the activities of its espionage network in Romania (Brestoiu and Bobocescu, 1979, p. 132).

Considering that the collaborator network of the German intelligence in Romania included people with important positions in the state (including the name of Alexandru Marghiloman, an important politician), the director-general of State Security, Iancu Panaitescu, forwarded the file stolen from the diplomat to King Ferdinand and Prime-Minister Ion I.C. Brătianu.

Although these discoveries required the taking of urgent organizational measures, given that the Transylvanian offensive was about to begin on the 15/28 august 1916, the immediate replacement of superior officers who had been proven to be enemy agents was no longer possible. To avoid the "demoralization of the army", the names of officers and generals who had betrayed in favor of the enemy, was not made public. However, their access to operational files was restricted and they were placed under surveillance until they could be eliminated from their positions and brought before a Court Martial. General Zottu was suspected of favoring the transmission of the Romanian Army's campaign plan for a war on the side of the Entente to the Central Powers. When he found out that their names was on the list stolen from von dem Busche, both general Zottu and major Ionescu, the Chief of Staff of the 2nd Army Corps killed themselves to avoid the expected interrogation, the public humiliation and the death sentence that was going to be issued (Ștefănescu, 2007, 45).

However, attempting to attract active or retired officers to commit subversive action by paying them was not an infallible method as is shown by a conclusive example which occurred in the beginning of the First World War.

Considering the extension of the conflict which had begun in the summer of 1914 (at that moment, none of the major powers involved did not expect that the war would become global in scale and would lead to the re-modelling of the world), both the Central Powers and the Entente try, under all possible forms, to sabotage the war effort of the enemy coalition. An interesting case, featuring the German ambassador von dem Busche, is pointed out by the agents of State Security.

The German Ambassador attempted to corrupt a reserve navy captain, Gheorghe Coandă, to undertake actions aimed at disturbing the Danube River traffic through which Serbia, a major Austro-Hungarian enemy, was supplied with military materiel (ANIC – DPSG, 177/1914, p. 1). The action aimed at sinking barges loaded with weapons and different military material which were loaded in the Russian port of Reni and unloaded on Serbia's territory. Mines necessary for the action would be given to the Romanian captain by the German official, and the former would plant them in the Danube's waters between Cernavodă and Galați.

Coandă requested that some money be paid as a deposit, as well as a 6000 lei down payment. However, after receiving the money, the captain contacted the Russian military attaché, colonel Semenoff, and suggested to organize a series of fake "attacks" against Russian transport ships. These ideas were not carried out (ANIC – DPSG, 177/1914, p. 8) and Germany ended up paying large sums of money without obtaining concrete benefits, while actions to block the Danube failed completely.

Another example, from a different vicinity of Romania and in a completely different context, points out to the universality of the financial motivation. In October 1917, the Bolshevik party succeeded in taking over power in Russia. Through its large intelligence network in the Bessarabian and Ukrainian communist movement, Romanian State Security was able to inform the Bucharest leadership about the plans and intentions of the communists. The elite group around the feared Cristian Rakovsky was penetrated. Rakovsky had established his general headquarters around Odessa, aiming to "ignite" the communist revolution, including in Romania.

A note labeled as maximum emergency, dated October 1917, included a report by the "Odessa Security Agent" (no details on his identity were mentioned): "I have been told by a person from Rakovsky's entourage, that the latter had sent a memoir to Petrograd, requesting a decisive action against Romania. Rakovsky and the Russian Jews are leading the plot

Two agents on my payroll in Rakovsky's entourage, would, for a generous amount of money, attempt to find out the intentions of the Jewish Committee and of its leader. One of them told me that he is ready to assassinate Rakosvky in exchange for an important sum of money.

Please urgently instruct me about the sum of money I could offer these people to stimulate them to give me information on Rakovsky's plot against the King and Government. Even an hour of delay could result in losing this opportunity" (ANIC – DGP, 3/1913, p. 48). Unfortunately, documents extant in the Romanian National Archives did not allow us to identify the end of the affair, but it is clear that there was no success in assassinating Rakovsky.

In archival documents, one can encounter examples of defection by professional military officers for "moral" reasons, due to their political-ideological convictions. In addition to the shock caused by the frontline defeats (which occurred in a very short time), as well as to the resulting evacuation to Moldova of Romanian state authorities, the betrayal of colonel Alexandru Sturdza, the son of well-known politician Dimitrie A. Sturdza and commander of the 7th Mixed Brigade, created significant commotion among Romanian troops (Otu and Georgescu, 2011). Colonel Sturdza deserted to Germany convinced that only an alliance with Wilhelm II's Reich could save Romania from occupation by the Tsarist Empire. State Security reports show that his action was not spontaneous, but had been planned well ahead.

Considering his decisions as a front-line unit commander, the colonel's desire to sabotage the intentions of State Security employees to send agents behind the German-Austro-Hungarian frontline: "Gheorghe Gherman, an inhabitant of Tulnici, Vrancea county, was sent by us across the mountains with specific requests that we had assigned, being recommended by Romanian military authorities. Colonel Sturdza, the commander of the 7th Mixed Brigade, informs us, through address No. 1062 of 20 November 1916 that, when Gheorghe Gherman requested to be allowed to cross the border, this was categorically refused, with the simple and naive reason that he is not trustworthy. As Gherman disappeared, Sturdza decided that he be found.

Colonel Sturdza, the commander of 7th Mixed Brigade, also informed us, through address no 1088 of 21 November 1916, that Gheorghe Gherman, after having clandestinely crossed the border, committed espionage in favor of the enemy and betrayed the movement of Russian troops to the Austro-Germans. Sturdza ordered that any person sent this way be arrested for lack of trustworthiness. The head of the Intelligence Bureau of the Northern Army, through address No. 62 of 2 December 1916, considering the case presented by Colonel Sturdza, forbids the Intelligence Center to send informers across the border. The intelligence center, based on official documents in the file, whose authenticity could not be denied by anybody, reported that all of colonel Sturdza's intelligence does not correspond to the truth" (ANIC – DGP, 16/1926, pp. 54-55v).

Sturdza's actions of sabotaging the national military effort would be completed through his crossing to the enemy side in the early morning of February 6th 1917, an action which led to major shocks across the army, as well as across Romanian public opinion. His enthusiasm quickly collapsed, as he was not successful in his propaganda among Romanians held prisoners in German camps, aiming at creating an "army" fighting against the Central Powers. This occurred despite the promises made to soldiers in very difficult situations, who, due to lack of food and exhausting work, were suffering thousands of casualties.

Conclusions

The main aim of this article was to apply models of analysis developed to study reasons for defection at a particular time and in a particular geopolitical context to a completely different context, in order to verify their validity. Through the study of Romanian historical sources from the time of the First World War, one can validate models developed 30-50 years later in the specific context of the Cold War. Employing these models allows for a novel approach to historical sources used, until then, in primordially descriptive ways. Thus, a new light on the universal phenomenon of defection is cast, given that it is susceptible of different manifestations according to the specific context and situation.

The article mainly employs the MICE (Money-Ideology-Compromise-Ego) model, also discussing its partial modifications. In the classic model, defectors are motivated either by money, ideology, blackmail or arrogance. This model was applied to spies captured in the United States, where the empirical study determined the replacement of the last two terms with motivations such as "divided loyalties", "disgruntlement" or "ingratiation".

A radical reconsideration argued for the replacement of MICE with the RASCLS model, which represented a considerable departure from the original.

Historical analysis of sources relevant for the period of the First World War in the Romanian area revealed radically different motivations for collaborating with enemy intelligence services. Firstly, when analyzing the activities of Romanian intelligence in Transylvania, at the time under the Austro-Hungarian Empire, strong "divided loyalties" were found among the ethnic Romanian inhabitants. Despite significant risks to their welfare, many of them engaged in espionage against their own state, offering crucial information to Romania. Austrian citizens of Romanian ethnicity were experiencing feelings of loyalty to Romania, something to which Hungarian assimilationist policies must have contributed.

On the other hand, the activity carried out by the Austro-Hungarian intelligence services on Romania's territory, as well as its conspicuous successes, must not be denied. Among the important sources of information that these services recruited were superior officers of the Romanian Army, drawn either by money or by the appeal of a superior culture, especially when weighed up against tsarist Russia, which was Romania's formal ally. Moreover, the communist movement represented a permanent source of concern for the Romanian authorities, considering that the inner circle of the revolutionary Rakovsky was penetrated by State Security agents, by relying on important sums of money.

The article's final conclusion is that, regardless of the applicability of one or another analysis model, the phenomenon of betrayal is universal, extending across time and space. Understanding the perennial motivations which determines it can help an intelligence service to protect itself from enemy intrusions and to also obtain success in its offensive operations against an enemy.

References:

1. Romanian National Archives, Collections - *Direcţia Generală a Poliţiei*, *Direcţia Poliţiei şi Siguranţei Generale*, *Ministerul de Război* (ANIC – DGP and ANIC – DPSG).
2. Brestoiu, Horia, Vasile Bobocescu, (1979), *Momente din activitatea organelor de ordine, informaţii şi contrainformaţii româneşti în perioada 1878 – 1918*, Serviciul Editorial şi Cinematografic, Bucureşti.
3. Burkett, Randy, An Alternative Framework for Agent Recruitment: "From MICE to RASCLS", *Studies in Intelligence Vol. 57, No. 1*, accesibil pe

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf, (accesat la 27.08.2015).

4. Charney, David L. și John A. Irvin *A Guide to the Psychology of Espionage,* accesibil pe http://www.afio.com/publications/CHARNEY_The_Psychology_of_Espionage_DRAFT_2014Aug28.pdf, (accessed at 22.08.2015).
5. Charters, David A. (2013) *"Have A Go": British Army/MI5 Agent-running Operations in Northern Ireland 1970–1972*, in *Intelligence and National Security*, 28 (2013):2.
6. *Din Memoriile lui Eugen Cristescu*, (1968), Consiliul Securităţii Statului, Direcţia Învăţământ, Bucureşti.
7. Crumpton, Henry A. (2013), *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*, New York: Penguin Books.
8. Herbig, Katherine L (2008), *Changes in Espionage by Americans: 1947-2007,* accesibil pe https://www.fas.org/sgp/library/changes.pdf, (accessed at 29.08.2015).
9. Lowenthal, Mark M. (2011), *Intelligence: From Secrets to Policy*, CQ Press: Los Angeles.
10. Mareşal Averescu, Alexandru, *Notiţe zilnice din război 1915-1918*, ediţia a III-a, Editura Cultura Naţională, Bucureşti.
11. Michalak, Sebastian, (2011), *Motives of espionage against one's own country in the light of idiographic studies*, in *Polish Psychological Bulletin, vol. 42(1), 1-4,* accesibil pe *http://www.degruyter.com/view/j/ppb.2011.42.issue-1/v10059-011-0001-2/v10059-011-0001-2.xml,* (accessed at 22.08.2015).
12. Neagu, C., D. Marinescu, R. Georgescu, (1977), *Fapte din umbră*, vol. II, Editura Politică, Bucureşti.
13. Otu, Petre, Maria Georgescu, (2011), *Radiografia unei trădări. Cazul colonelului Alexandru D. Sturdza*, Editura Militară, Bucureşti.
14. Pertman, Adam (2001), *Why They Spy Be It Ideology, Ego or Disaffection, Almost Always a Thread Connects Motive and Money*, 25.02.2001, accesibil pe http://fas.org/sgp/news/2001/02/bg022501.html, (accessed at 1.09.2015).
15. Project Slammer interim report, 1996 http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000218679.pfd (accessed at 1.09.2015).
16. Shapiro, Shlomo (2011), "KGB Human Intelligence Operations in Israel 1948–73", *Intelligence and National Security*, 26:6.
17. Stein, Jeff Wikileaks: CIA studied why people steal secrets, 06.07.2010, accesibil pe http://voices.washingtonpost.com/spy-talk/2010/06/wikileaks_cia_studied_why_peop.html, (accessed at 20.08.2015).
18. Stone, Leroy (1992), A principal component analysis of 59 variables of uncovered spies" în *34th Annual Conference of the Military Testing Association, Proceedings,* Volume II, Octombrie 1992,

http://www.dtic.mil/dtic/tr/fulltext/u2/a268816.pdf, (accessed at 1.09.2015).

19. Ştefănescu, Paul (2007)*, Istoria serviciilor secrete române*, Editura ANTET, Prahova.
20. Taylor, Stan A. şi Daniel Snow (1997), *Cold war spies: Why they spied and how they got caught*, in *Intelligence and National Security*, 12 (1997):2, 101-125.
21. Thompson, Terence J., (2014), Towards an Updated Understanding of Espionage Motivation", *International Journal of Intelligence and CounterIntelligence*, 27:1, 58-72.

REVIEWS AND NOTES

ROMANIAN PUBLICATIONS ON BUSINESS INTELLIGENCE - LITERATURE REVIEW BY OANA PUIE (ANIMV) -

The dynamic evolutions of the national and global security environment have determined the adaptation and reconfiguration of government intelligence. Starting from the same pattern, unpredictable fluctuations in the business environment have led to the development and use of common practices related to business intelligence. This adhesion to current information needs to become visible in both the current practices of companies and in the field of publishing. Thus, amid a growing information need, the importance and impact of specialized journals has increased, namely of those publications addressing issues regarding the scope of its business intelligence and other related topics.

The purpose of this review is to bring forward the short presentations of two such periodicals published recently in the Romanian publishing environment: *Business & Competitive intelligence. Business Intelligence Review* and *Network Intelligence Studies.*

Such publications enhance the knowledge and awareness degree of new challenges in the field of business, and also give access to debates and researches on issues of current interest. On the one hand, publishers and authors that work in a collaborative environment are able to express hypotheses and to argue them in a relevant way, enriching the fund of knowledge and understanding of developments in the field of business intelligence. On the other hand, readers are familiar with perspectives and visions filtered by personal attitudes and tailored according to specific contexts that can turn into opportunities for development and promotion.

Business & Competitive intelligence. Business Intelligence Review is the official publication released by the Association of Specialists in Business Intelligence (ASIA), available on the website http://asia.org.ro/html/revista.html.

Despite its limited publication – only 6 numbers between 2012-2013 –, it stands out among the first specialized publications in the field of business intelligence. With a bilingual appearance, the review aims to contribute to the objectives of the Association: "developing the area of business intelligence" (Business & Competitive Intelligence), development area "Information for Business" (Business & Competitive Intelligence), thereby increasing the competitiveness of companies in our country – (http://asia.org .com/ Macheta_BI-CI _-_ Nr.1.pdf). According to the opening speech, the team around the Association and the review "brings together experts and practitioners from business and academia, willing to define and ensure the necessary professional landmarks, that should become a reference to all those who want to know and to use in a systematic way business information in order to increase performance" (http://asia.org.ro/Macheta_BI-CI_-_Nr.1.pdf).

Network Intelligence Studies (NIS), available at http://nis.bxb.ro/, is a publication specialised in the study of intra and inter-organizational collaborative networks. Under the aegis of the Romanian Foundation for Business Intelligence (Romanian Foundation for Business Intelligence, see details at http://bxb.ro/) and under the coordination of the Business X Business Department (bxb), the review is published twice a year, the first issue going back to 2013.

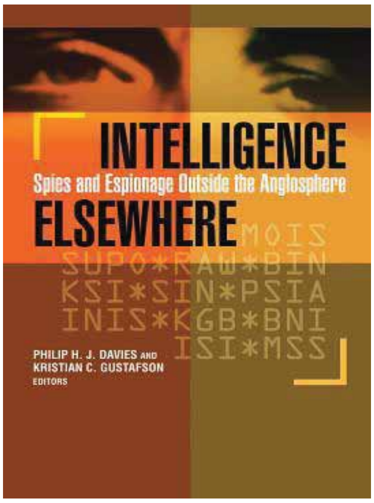
From a technical standpoint, it is conceived as a whole, as a 2-number volume is published every year. The NIS editorial meets cooperation and support needs between individuals, companies, universities, non-governmental organizations and communities, in order to generate useful results that can subsequently substantiate beneficial decisions.

According to a clearly stated vision, the mission of the journal is to create a research and learning platform that would enjoy the participation and interest of both the academic and economic community. Thus, through the participation of interested contributors and readers, stimulating discussions on topics related to the field of business intelligence, focusing on the importance and impact of collaboration in this area. Articles are signed both by Romanian and foreign authors, the result generating a mix of perspectives and approaches that support the idea of interculturalism promoted by the editors. Articles are the product of the collaboration between people from academia, the economic environment or national administration, as well as specialists from various spheres, from countries such as India, Italy, USA and Hungary.

Readers are offered a wide range of topics that transcend the sphere of theoretical business intelligence and approach issues related to intercultural innovation and inter-organizational elements of management theory, entrepreneurship and international business, anthropology, intercultural performance, the methodology of intercultural training, measurement and growth of the economic performance, economic, social, political and security impact of various global changes.

In conclusion, the two publications provide the possibility to access more than just business intelligence information, as they can be seen as an open platform that mediates collaboration on multiple levels between education, research, economy and private business. Regardless of the themes, the major advantage of the two publications is that they have a general application and can even be a starting point in the study and academic research in the field of business intelligence or business development and improvement. Publishing articles in English complements the idea of interculturalism and facilitates access to a wide audience, beyond national and linguistic borders.

PHILIP DAVIES ȘI KRISTIAN GUSTAFSON EDITORS, (2013), *INTELLIGENCE ELSEWHERE: SPIES AND ESPIONAGE OUTSIDE THE ANGLOSPHERE*, GEORGETOWN UNIVERSITY PRESS, WASHINGTON D.C. REVIEW BY COSMINA-ELENA EPURE (ANIMV)



The volume entitled *Elsewhere Intelligence: Spies and Espionage Outside the Anglosphere* is structured as a complex collections revolve around a single pole: intelligence. Its authors, Philip Davies and Kristian Gustafson, known as the personalities involved in the field, harness a series of works and references of several specialists with the aim of building a broad vision on what intelligence represents.

Scientific contribution is even greater as we witness an academic approach focused on two levels: the historical dimension – a pillar in the construction and development of concepts and ideas and present, focusing on the political and cultural contexts.

Historical perspective. Knowledge starts by taking a look at the origins, therefore the intelligence community historical perspective is fundamental to determining the present and the future. In this sense, the authors resort to comparative analysis of the role of culture in intelligence, with a stop at a few examples: India, China, the Arab world and Russia. It is emphasized the importance and timeliness of the work of Sun Tzu, by the fact that at the core of Chinese armed interventions is subversion and espionage. As regards Russia's acting, it is a comparison between the Byzantine Empire forecasts and the Soviet period. The conclusion to this example marks the importance of the Byzantine period in the democratization of Russian intelligence practices.

The chapter on the Arab world places clandestine intelligence gathering and espionage in Islamic and Arabic history, specifically the period the prophet Mohammed tried to maintain his religion emerging.

Current perspective. The second part of the book is dedicated to an particular analysis of each state regarding current practices in intelligence and also the needs and requirements in order to change and to adapt to policy makers and to the security environment.

If we are to talk about Pakistan, its domestic intelligence services exercise a strong influence on the state. Iranian intelligence activity is the result of an interaction between three factors – Shi'ism, bureaucracy, and clerical factions. Political privileged consensus on informing decision makers is one that revolves around what it is targeting Japan in intelligence. This contributes profoundly in affecting the proper conduct of the intelligence process.

Next three chapters follow the reform of the security sector and are invoked as examples Ghana, Argentina and Indonesia. It is stated, in this case, approaching practices and measures in intelligence is closely linked to Eastern European experience.

As a novelty, the authors dwell on issues that have not been exploited out regarding intelligence field. Thus, it is about Northern states that take into consideration different strategies than European ones. In support of this assertion is Sweden, characterized by bureaucratic tradition and socialist tendencies. For its part, the intelligence work was conducted independently.

Both Sweden and Finland evaluate their orientation and priorities in the post-Cold War world, noting that tend towards different directions due to historical, economical and security interests, but also extremely important – thanks to strategic culture.

Conclusions. The starting point of the intelligence activity is the uncertainty. Starting from a base so unstable, in a continuous change, the authors admit a disadvantage of this type of activity: it can not be considered as being always truthful.

But the worth of intelligence activity lies on the attempt to limit or reduce uncertainty. Therefore, through the collection, processing and analysis of information can build some solid insights that contribute to decision making process in a state, as well as maintaining and safeguarding national security interests.

Knowing the purpose of an intelligence service, we can move on to particular elements of each state – the first and most important is culture, which is under the umbrella of specific tradition and heritage (eg. Pakistan and Indonesia where Sanskrit tradition is highlighted).

Achieving an intelligence service objectives is to apply the techniques and methods that characterize it. In this section, the authors launches dyad covert actions – diplomacy. Therefore, history places in the same area espionage, sabotage and assassinations, while reality suggests lack of violence as a management dimension of foreign policy – diplomacy. The passage of time is the factor that has contributed to the evolution of intelligence and how it can be applied.

In the academic approach, the work of Philip Davies and Kristian Gustafson comes as a cornerstone of the knowledge and deepening of the area of intelligence. In this respect, the fundamental role of history and tradition that is assigned to act as a fingerprint on the present and current practices. However, the volume is a part of an attempt to define intelligence studies as an academic discipline.

The greatest achievement of this volume lies in forgetting for a moment the espionage world consisting of only United States of America, United Kingdom and Europe. Therefore, the two authors establish that in the academic research of intelligence, knowledge can't rest on a niche level.

This collection of scientific papers can be treated as a great opportunity to find an universal framework in order to define intelligence and its techniques and methods. Besides all this, an aspect that lacks approaching is the dimension regarding national intelligence implementation in each country and also the relation with decision makers. Consequently, it appears a need to deepen the research and, in this way, to create a wider vision (which can represent the base for comparative studies).

Taking into consideration the constantly changing security architecture as well as changes occurring in the international distribution of power, "Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere" provides basic knowledge for a better understanding of current and future events .

A well-known quote of Nicolae Bălcescu, *"The history is the first book of a nation. Within it past, present and future can be seen"* gives a good conclusion that every process or research, irrespective of its nature, involves taking a look into history. In this instance, intelligence area is in a permanent development and to underlie studies and ideas, the past plays and important part. The purpose is to come with a forecast related to reality which becomes a benchmark in developing policies and strategic decisions.

ACADEMIC FOCUS

TWELTH ANNUAL IAFIE CONFERENCE AND FIRST ANNUAL CONFERENCE OF IAFIE'S EUROPEAN CHAPTER IN BREDA, THE NETHERLANDS JUNE 22-24, 2016

Leading international organization for Intelligence Education, IAFIE was formed in June 2004 as a result of a gathering of 60 – plus intelligence studies trainers and educators. Coming from various intelligence disciplines including national security, law enforcement and competitive intelligence, they recognized the need for a professional association that would span their diverse disciplines and provide a catalyst and resources for their development and that of Intelligence Studies.

The mission of the Association is to advance research, knowledge and professional development in intelligence education by:

- providing a forum for the exchange of ideas and information;
- fostering relationships and cultivating cooperation among intelligence professionals in academia, business, and government;
- developing, disseminating, and promoting theory, curricula, methodologies, techniques, and best practices for pure and applied intelligence;
- serving as a liaison between other professional organizations and centres of excellence;

Already a tradition, the annual IAFIE Conference will focus next year on Connecting Intelligence Education Communities: Europe, North America, and beyond, and will be held in Breda, the Netherlands, between June 22-24, 2016. The European Chapter will gather scholars and practitioners from various national Intelligence communities in a two day conference with six key-note speakers and no less than 24 workshops.

With a variety of keynote speakers and a broad array of panels, the IAFIE conference intends to further explore current questions for the Intelligence field and provide the beginning of an answer to them, thereby contributing to both the public understanding of intelligence and the quality of intelligence teaching and practice. Further information about IAFIE membership, projects and details of conference can be found at www.iafie.org

„SECURITY IN THE BLACK SEA REGION. SHARED CHALLENGES, SUSTAINABLE FUTURE” (SBSR) THIRD EDITION BUCHAREST-SIBIU, May 30 – June 4, 2016

The Romanian Intelligence Service, organizes, during May 30th and June 4th 2016, via its National Intelligence Academy, the third edition of the international program “Security in the Black Sea Region. Shared challenges, sustainable future” (SBSR). The program has been developed in partnership with Harvard University and with the participation of National Intelligence University (US).

Carried out under the auspices of the Romanian Presidential Administration, SBSR takes on the philosophy, mission and goals of the Regional Black Sea Security Program (BSSP), which was initiated by Harvard University 15 years ago. The current program also embraced the mission to promote and enhance regional actors' responsibility and initiative in approaching security challenges in the Black Sea Region. **The third edition focuses on “Convergent forms of power in the Black Sea Region. Think hard, act smart”.**

The Black Sea Region has witnessed in recent years dramatic shifts in the balance of power. While the sovereignty and democratic development of the countries in the region have been placed under pressure by confrontational geopolitics, hybrid warfare, global terrorism or, at times, internal corruption and political imbalances, actionable responses have become a critical factor in addressing regional security. Therefore, the new ecology of power, which is significantly different from that experienced a decade ago, speaks of an increasing need to reframe and map out national interests, interconnect regional alliances and improve complex interdependences. It is in this context that we would like to dedicate the 2016 edition of the “Security in the Black Sea Region. Shared challenges, sustainable future" Program to debate current convergent forms of power in the Black Sea Region and their impact in creating the right tools for confict resolution and sustainable development throughout the region.

This year's edition will be honoured by keynote speakers and participants from Armenia, Azerbaijan, Bulgaria, Canada, Germany, Georgia, Greece, the Netherlands, the United States, the Russian Federation, Moldova, Romania, Turkey, and Ukraine, as well as high ranking officials and experts from the European Union and NATO. For more details please visit http://www.sbsr.ro.

INTELLIGENCE IN THE KNOWLEDGE SOCIETY THE 22nd EDITION BUCHAREST, OCTOBER 13-14, 2016

Intelligence and security studies and their instrumental use by practitioners remains a constantly changing and challenging endeavor, requiring interdisciplinary perspectives. *Therefore* We invite academics, experts and practitioners from the classical disciplines of intelligence and security studies as well as e.g. IT&C, law, mathematics, social sciences and humanities to offer insights derived from each's discipline.

The 22nd edition of the anual International Conference Intelligence in the Knowledge Society (IKS) aims to explore multi and inter-disciplinary perspectives on the interaction, intersection and interdependence between the exponentially growing new technologies, security and intelligence.

The security studies section of the conference, The future world(s) of security, welcomes specialists from various fields to study by reflecting on core themes like: revolutions of community thinking and power structures – implication for national security; new forms of good governance, active citizenship and collective security; information and communication technology; Connectivity, wellbeing and surveillance; bioengineering the future of security; belonging, conflict and the weaponization of identity; identity, allegiance and the security implications of multiple loyalties; understanding history, understanding the future past of our secure environment.

Intelligence at a crossroads, the intelligence studies section of the conference, welcomes specialists from various fields to study by reflecting on core themes like: intelligence as a process, activity, product; intelligence education between the need for secrecy and the competitive advantages of openness; transformations of the organizational culture of intelligence agencies; the Cinderella complex of intelligence analysists; technological evolution – amplifying knowledge or vulnerability in intelligence practice; patterns of accelerated evolution vs. systematization of intelligence practice.

The conference will also explore ways in which intelligence and security methods and practices need to be reshaped to address the challenges of asymmetric, smarter, better and faster aggressors. Controversial topics, innovative solutions, best practices and challenges to be overcome will be addressed in an interactive manner by key note speakers and participants alike. For details please visit the site http://www.intelligencestudies.ro

CITYCOP
CITIZEN INTERACTION TECHNOLOGIES
YIELD COMMUNITY POLICING
June 2015 - May 2018

"Mihai Viteazul" National Intelligence Academy (MVNIA) is partner in CITYCoP project, being responsible with the training program design.

Theories underlying community policing received new impetus with the recent advent of smartphones and social media and especially user-generated content (UGC) where citizens engage in closer interaction with their local community and law enforcement agency (LEA)

The years 2010-2014 have seen a rapid upsurge of smartphone apps aimed at improving crime reporting and other forms of UGC and interaction associated with community policing. Yet these apps are characterised by a predominantly Anglo-Saxon approach with the largest number originating in the USA, a few in Canada, Australia and with the UK apparently the only major EU state where there has been some take up of these technologies.

CITYCoP sets out to find out why the EU appears to be lagging behind although Community Policing is nominally a policy which has been put into action in a number of EU countries. It then goes on to develop a solution including a new smartphone app and on-line portal which are capable of being deployed in any European city while still retaining "local flavour" and diversity. These ICT solutions will also be designed from scratch to be fully compliant with strict privacy and data protection laws. A training scheme, including use of serious games, will be developed to assist training of officers and citizens in use of the app and portal.

CITYCoP will benefit from a multidisciplinary approach that will include the sociology of community policing as well as cognitive science perspectives of the citizen's interaction with community and LEAs through technology. CITYCoP involves 22 institutions from 13 countries and has been awarded with EU Horizon2020 funding. The partners in CITYCoP build on long years of successful collaboration in EU projects dealing with UGC, smart surveillance and privacy (CONSENT, SMART, RESPECT) positioning CITYCoP solutions to achieve integration into smart city eco-systems. CITYCoP will pilot deployments of multi-lingual smartphone apps, portals and serious games training packages in Bucharest (Romania), Lisabon (Portugal), Florence (Italy), and Sheffield (UK).

CARISMAND
CULTURE AND RISK MANAGEMENT IN MAN-MADE AND NATURAL DISASTERS
October 2015 - September 2018

"Mihai Viteazul" National Intelligence Academy (MVNIA) is partner in CARISMAND project, being responsible with the research of risk perceptions in different cultural contexts and crises.

As risks are not "objective" but socially and culturally constructed, disaster management which is aware, respects, and makes use of local cultural aspects will be not only more effective but, at the same time, also improve the community's disaster coping capacities.

CARISMAND is setting out to identify these factors, to explore existing gaps and opportunities for improvement of disaster policies and procedures, and to develop a comprehensive toolkit which will allow professional as well as voluntary disaster managers to adopt culturally-aware everyday practices. This goal will be achieved by approaching the links, and gaps, between disaster management, culture and risk perception from the broadest possible multi-disciplinary perspective and, simultaneously, developing a feedback-loop between disaster management stakeholders and citizens to establish, test, and refine proposed solutions for culturally-informed best practices in disaster management.

Whilst experts from a variety of fields (in particular legal, IT, cognitive science, anthropology, psychology, sociology) will undertake a comprehensive collation of existing knowledge and structures, a number of Citizen Summits and Stakeholder Assemblies will be organised. Systematically, CARISMAND will use an approach that examines natural, man-made and technical disasters, placing at the centre of attention specific aspects that affect culturally informed risk perceptions, eg whether disasters are caused intentionally or not, the different "visibility" of hazards, and various time scales of disasters such as slow/fast onset and short- and long-term effects.

CARISMAND involves 19 institutions from 14 countries and has been awarded with EU Horizon2020 funding. By organising six Citizen Summits (two per disaster category per year in two separate locations) where such disaster risks are prevalent, and three Stakeholder Assemblies (one per year) where the results are discussed through a wide cross-sectional knowledge transfer between disaster managers from different locations as well as from different cultural backgrounds. The “Mihai Viteazul” National Intelligence Academy will co-ordinate a Work Package that relates to the part of the project that deals with risk perceptions in the context of cultural factors, man-made and natural disasters.

SAFFRON
SEMANTIC ANALYSIS AGAINST FOREIGN FIGHTERS RECRUITMENT ONLINE NETWORKS 2015-2018

The "Mihai Viteazul" National Intelligence Academy is part of the SAFFRON project – *Semantic Analysis Against Foreign Fighters Recruitment Online Networks* – that is financed by the European Commission through the Program Preventing Radicalisation to Terrorism and Violent Extremism.

The conflict in Syria may be the first conflict in which a large number of Western fighters have been documenting their involvement in conflict in real-time, and where – in turn – social media represents an essential source of information and inspiration to them. Analysing the recent trends about recruitment of foreign fighters by terrorist groups, and comparing online communication strategies, the SAFFRON project observe the development of a bottom-up social media strategy, which facilitates the progression of the individual from non-violence into violence.

Considering the increasing role the social media plays in the online recruitment and radicalization of foreign fighters, the project aims at developing a test tool capable of identifying in a timely fashion manner all internet activities pertained to online radicalization and all signals pointing at radicalization of single individuals.

REACT
PN-II-RU-TE-2014-4-1669
SOCIAL PERCEPTION AND COMMUNICATION STRATEGIES IN RISK PREVENTION. A NATIONAL SECURITY PERSPECTIVE ()
October 2015 - September 2017

Social perceptions and communication strategies in risk prevention. A national security perspective is a project supported by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS – UEFISCDI implemented by "Mihai Viteazul" National Intelligence Academy through the National Institute for Intelligence Studies.

The management of and communication about risks has become a major question of public policy and intellectual debate in the modern world. Risk perception analysis focuses on subjective judgments that people make about the characteristics and severity of a particular risk. Our research project proposes the use of qualitative research methods (Q sort method) in order to measure and define Romanians' knowledge, attitudes and practices regarding national security risks.

In order to improve our capacity to prevent, prepare and respond to major national security risk, we want to answer the following key questions: What is the level of knowledge on national security risks in the Romanian society? What are the main concerns of Romanians? What information does the society need regarding this risk?

In this respect, the main objectives of our research are:

1. Analyse and understand the limits of the current risk management and risk communication strategies, through a content analysis of the strategic documents elaborated by national security institutions.

2. Improve our understanding of how people perceive and act in relation to risk. Having greater knowledge in the field of social risk perception can thus improve the quality and impact of decisions throughout society, and the quality of risk communication strategies.

3. Provide a new perspective over the social risk perception in Romania, by suggesting an alternative method for measuring risk perception (Q sort method).

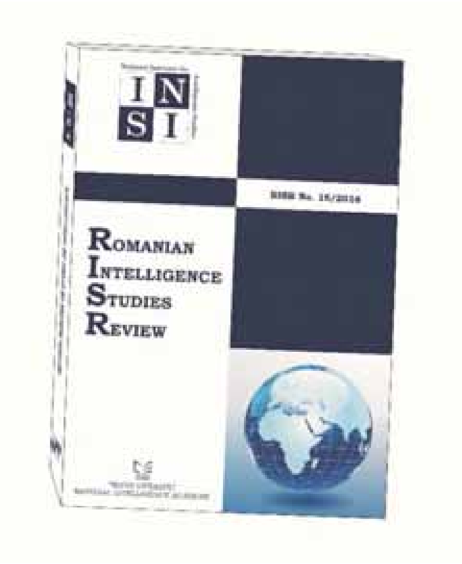
Therefore, the objective of our research consists in the elaboration of some solutions for the optimization of the management of security risks and communication strategies for national security institutions, through the analysis and evaluation of social perception over national security risks.

REACT project aims to improve the research skills on risk perception of the research team members through their involvement in conducting sociological research in a relatively new field at national level: social risk perception analysis. The research is focused on identifying patterns among the different variables (respondents) for each subject analysed (statement) and on finding evidence to prove there is a connection between the performances of the two variables. Taking this into consideration, the Q-sort methodology provides a basis for the systematic study of subjectivity, of points of view, opinions, convictions, attitudes towards national security risks.

Beyond the academic contribution to the study of national security risks, we intend to provide an assessment of the perception of national security risks by the Romanian society, by conducting a research using the Q-sort method on a sample of individuals from the academic, private, civil society and institutional (national security institutions) environment.

We may conclude that our project has a political, economic, cultural and social impact, it contributes to the reduction of the gaps in knowledge in the field of intelligence analysis between Romania and other European states, to the reduction of the people’s vulnerability and to an increased resilience towards national security risks.

CALL FOR PAPERS
RISR no. 15/2016



"Mihai Viteazul" National Intelligence Academy, via its National Institute for Intelligence Studies, publishes the Romanian Intelligence Studies Review (RISR), a high quality peer reviewed and indexed research journal, edited in Romanian and English twice a year. Submission deadlines are February 1st and July 1st. Authors interested in publishing their paper in RISR are kindly invited to submit their proposals electronically in .doc/.docx format at our e-mail address rrsi@sri.ro, with the subject title: RRSI article proposal.

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy
- Intelligence in the 21st century
- Intelligence Analysis
- Open Source Intelligence (OSINT)
- History and memory in Intelligence

RISR shall not accept or publish manuscripts without prior peer review. Articles will be selected based on their relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area.

Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and http://www.animv.ro for author guidelines.

PEER REVIEW BOARD