TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 8, 2020

A new decade for social changes

ISSN 2668-7798

www.techniumscience.com

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

Views on technology development and transformation into Intelligence

Tănase Tiberiu[1], Nagâț Violeta Ioana[2]

[1]Romanian-American University of Bucharest, Romania, [2]PhD. Student -Academia de Informații "Mihai Viteazul", Bucharest, Romania
tiberiu_tanase@yahoo.com[1], vio_nag@yahoo.com[2]

Abstract. During recent years the international environment has shown an increasing instability and more dangers and threats. All actors have to adapt their strategies to this new context, for being prepared to compete successfully with. In these conditions, intelligence's role is to prevent threats deriving from the use of new technologies. One way of doing that consists in the transformation process of intelligence. Intelligence has to adapt to new challenges so as to provide policy makers and military information in order to make decisions for countering the cyber threats.

Keywords. cybersecurity, challenge, vulnerabilities, risks, threat, aggressions, intelligence

Introduction

The 21st century is marked by profound transformations of the security environment. The emergence of a global economy, strongly interconnected, reconfigures the system of international alliances, accelerates the adoption of technologies and enhances the development of new economic centres. This interconnected world offers new opportunities, but it also develops significant risks for international security, factors that will represent the coordinates of the new requirements for intelligence services.

Therefore, the transformation implies changes in the doctrines, the intelligence activity and the adaptation of the intelligence services to the current and future challenges, also setting the context and coordinates of the analysis framework: the fluid and increasingly changing security environment in the face of new challenges, but especially those that generate risks, the vulnerabilities generated by the phenomenon of rapid globalization, and not least the need to protect the national interest and the flexible and efficient functioning of intelligence services in the context of new security challenges - economic and financial crisis, pandemics or climate change, as well as their consequences.

Development of technologies for intelligence

Today, professionals in security will have to accumulate scientific, educational and commercial advantages to undermine opponents' ability to acquire and use cyber-attacks capabilities. The development of new microelectromechanical machines, nanotechnology discoveries, bio weapons, super-automated capabilities and artificial intelligence will be

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

applicable in the fields of security, intelligence, but also in military one. These developments may, on the one hand, improve the operational capabilities of intelligence services, the armed forces and security, but on the other, they may represent new threats from adversaries.

The development of technologies has led to an evolution of risk factors for the security of states and citizens, which has greatly influenced the adaptation of intelligence services to the security environment, mainly through their transformation and modernization, both on the operational component and on the analysis. In this context, cyber intelligence has become a component of security, especially on the line of protecting critical IT infrastructures, and cooperation between state institutions or with external partners, companies and non-governmental organizations, a necessary condition for promoting an adequate response to this new type of security challenges.

The globalization of communications and the exponential development of technologies have led to the manifestation of "classic" security risks in a new, virtual environment: from organized crime and computer crime networks, to electronic espionage or to multiplying terrorist action capabilities by using the Internet as a radicalization vehicle or preparation of extremist groups.

Another effect of the technological revolution was the increment of civil and commercial surveillance capabilities (satellites, GPS systems), which led to the need for a better integration of intelligence information with those from the private environment, which in turn the level of international politico-military organizations was conceptualized by the term *"intelligence fusion"*[1].

When the US and coalition forces were deployed to Afghanistan in search of Osama bin Laden, at the end of 2001, they were backed by an impressive range of aeronautical intelligence gathering platforms. These included E-3 Airborn Warning and Control Systems (AWACS); modernized U-2 surveillance aircraft; RC-135 Rivet Joint Sigint aircraft; E-8C Joint-Stars radar surveillance aircraft; Navy EP-3E Aries SIGINT and Navy EA-6B Prowler aircraft. But the US has also positioned nearly 50 satellites to support Operation "Enduring Freedom" in Afghanistan, many of which are dedicated to gathering information, illustrating their importance in collecting and disseminating information[2].

To understand the role that satellites have and what role they will play in collecting strategic information, we present four categories of satellites, which are currently used by the United States. First, there are satellites equipped to produce images under light, radar or infrared reflectance. A second category of early warning satellites is designed to detect ballistic missile launches. These include *Defence Support Program (DSP)* satellites and the former Infrared Space System (SBIRS), which have greatly increased the ability of the US to detect and intercept ballistic missiles, while adding intelligence gathering and characterizing combat space to the warning early function DSP satellite. A third category produces ***Signal Intelligence (SIGINT)***[3] and Electronic Intelligence (ELINT) by monitoring radio and electronic signals.[4] Throughout

[1] Matei Mihaela, Transformation of intelligence systems and the modernization process of the Romanian Intelligence Service, Intelligence Magazine no. 25 of September 2013, p. 40-43.
[2] Alan Dupont, Intelligence for the twenty-first century, în Intelligence and National Security, no.4/2003.
[3] Signal Intelligence (SIGINT) is intelligence gathering by intercepting signals, whether it is human communications (communication information - shortened by COMINT) or electronic signals that are not directly used in communication (electronic intelligence - inhabited by ELINT)- https://en.wikipedia.org/wiki/Signals_intelligence
[4] Electronic intelligence (ELINT) is the information collected through the use of electronic sensors. In ELINT, the information gathered is generally other than personal communication. The purpose is often to ascertain the capabilities of a target, such as the location of the radar. The sensors used to collect the respective data can be active or passive. A given signal is analyzed and compared to the data recorded for the known signal types. If the signal type is recognized, the respective information can be recorded; it can be classified as new if no match is returned. The data collected by ELINT are generally classified.- https://whatis.techtarget.com/definition/ELINT-electronic-intelligence

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

the Cold War, the US has used a series of SIGINT and ELINT collection satellites that have steadily increased in capacity, sophistication, weight and cost with each generation. A fourth group is that of satellites equipped with sensors that measure seismic, acoustic, chemical and biological fingerprints.

Known as ***Measurement and Fingerprint Intelligence or MASINT***, these satellites can detect traces of chemical agents and biological warfare or clandestine nuclear tests. With the proliferation of weapons of mass destruction, fears have been raised about the possibility of failed or terrorist states acquiring nuclear, biological and chemical weapons, which will lead to an intensification of MASINT's role. MASINT tries to extract the security information from any element that can be scientifically measured: radio waves, acoustic signals, nuclear radiation, infrared radiation, radio frequencies, electromagnetic pulse, liquid or solid waste, chemical composition, biological structure, material properties and so on (Making The Most of MASINT and Advanced Geospatlal Intelligence, Major Connie Lynn, USAF). The diversity of sources that can generate useful data in the intelligence process is reflected by the numerous sub-domains of MASINT: Radar Intelligence (RADINT), Acoustic Intelligence (ACOUSTINT), Nuclear Intelligence (NUCINT), Radio Frequency / Electromagnetic Pulse Intelligence (RF / EMPINT), Electro -Optical Intelligence (ELECTRO-OPTINT), Infrared Intelligence (IRINT), Laser Intelligence (LASINT), Unintentional Radiation Intelligence (RINT), Materials Intelligence etc.[5]

Also as a reflection of the technological development, which has supported the action of the intelligence services, the US use of ***UAVs (Unmanned Aerial Vehicle)*** is noted. The Predatory model has proven to be extremely valuable as an information collector and direct executioner of some strikes against Islamist leaders in Afghanistan and Pakistan. The predator can remain on the target area for about 20 hours, rendering SIGINT and IMINT data via satellites directly to the ground. A new generation of UAVs, Global Hawk, has been designed to be an "electronic vacuum cleaner" and to collect a variety of signals and emissions

Despite the special technological development, human spies, which produce *Human Intelligence or HUMINT*[6], are still indispensable to the information gathering activity despite the impressive advance of the technical means of collecting information. This conclusion was confirmed by the events of September 11, which signalled to the US intelligence community that, no matter how large is the amount of developed technology, it cannot compensate for the HUMINT quality.

It is true that much of the information collected by field agencies is derived from, or transmitted by, technical systems or devices that can rival satellites and UAVs, with all their sophistication and discretion. These include state-of-the-art audio and video surveillance equipment, frequency jump communication systems and the use of computer-generated random encryption. HUMINT has always made a very valuable contribution, but reduced in volume to the complete product of Western intelligence communities. However, as in other cases, the tasks and the operation of human agents are constantly changing due to technologies and changing priorities.

The use of technology, beyond its clear advantages in the information business, has proved, however, limiting by its effects: in the public debates about the failure of the American intelligence community in the case of Iraq's intervention, it has been revealed that the technical

[5]Adrian Robu The image of the threat. Sensors, sources of knowledge - Intelligence Magazine, 30 March 2020 https://intelligence.sri.ro/imaginea-amenintarii-senzorii-surse-ale-cunoasterii/
[6] HUMINT (Human Intelligence) is the activity of obtaining information from human sources

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

sources, however efficient that is, they cannot be a palliative for human secret sources and only their integration provides a correct picture of risk developments.

No amount of raw data can substitute for a keen analyst capable of distinguishing the sensitive aspects or the operational significance of an event, action or trend, which could be hidden in a mass of confusing and contradictory information.

Major failures in intelligence generally had a lack of information. These are often failures of analysis and sometimes of dissemination. But in the future, they could also result from overloading with information. The CIA acknowledged that the delay in recognizing that Iraqis were storing chemical weapons at Khamisiyah in 1997 was caused by the management problems of the vast amount of information available in the US intelligence community.

Given the availability of a vast amount of information, classified and unclassified, the task of the intelligence analyst will be increasingly difficult, choosing, organizing and evaluating them represents a major challenge for even the most informed and agile minds of the analyst.

The development of technology, especially the information technology, has influenced the increasing and real-time access to information, an evolution known as the OSINT "revolution": open sources of information, mainly through media channels, represent an extremely important capability for intelligence work and for the formulation of policies in the field of state security.

OSINT (Open Source Intelligence) is the result obtained by collecting and analysing data from open sources, such as the press, internet, ***scientific papers, legislative resources, images or publicly available video materials. According to the "NATO Open Source Intelligence Handbook"***, OSINT products compensate for the need for secret information[7]

The use of open sources cannot compensate for the typical activity of an intelligence service with secret sources, but it contributes more and more to the configuration of perceptions and to the understanding of phenomena at the level of intelligence analysis.

OSINT's role within it has grown exponentially in recent years, with many information services developing dedicated structures for this type of information. These developments have contributed to the gradual transformation of the classical concepts of intelligence and the definition of new frameworks for intelligence services.

On the other hand, another challenge for intelligence services is presently, the unprecedented expansion of communications networks, mainly determined by the multitude of attractive network services made available to users, miniaturization and the affordable price of storage, processing and storage resources, processing and information, simplicity of use of high-performance computer equipment and software, as well as the increasing number of users.

Thus, many vulnerabilities in communications networks are easy to exploit, and people and organizations everywhere can connect to these networks, beyond national borders. Also, the information technology makes it easy to hide the place and identity of the individuals and organizations that take advantage of these vulnerabilities

At the same time, new vulnerabilities of the networks are being permanently discovered and exploited. The interconnection of networks and the increasing dependence on these infrastructures make network activity an attractive prospect for hackers and those dealing with information gathering.

This gives rise to an asymmetrical challenge. The use with bad faith of information technology, if the economy or the state of security of the population is affected, causes the profile of the cyber-attack to *sometimes have features of terrorist action (cyber terrorism).* Cyber terrorism *consists of cyber-attacks that use the computer and the communications*

[7]SRI , OSINT Guide

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

network to cause significant harm, to create fear or to intimidate society for an ideological purpose. According to the FBI, cyber terrorism is defined as *the use of resources in the field of communications and information for the purpose of intimidation or coercion of others*[8].

Security IT incidents occur equally in classified and sensitive networks, as well as in public ones. The first category includes some government networks or belonging to state or private organizations, as well as international networks of NATO, EU or other organizations. In the category of public networks, the Internet is the most representative and largest network, becoming a global structure that connects millions of networks, hundreds of millions of personal computers, and a lot of devices. This global network has a decisive role in the efficient functioning of the various authorities: business, banks, trade, public administration and national security.

The new performance of information technology, of which we mention virtual networks, service-oriented architecture, cloud computing, grid computing, offers a wide openness, providing more and more services, which are attracting more and more users. But the advantages of this ever expanding architecture for the benefit of the users, of the information circulation also face a disadvantage: weakening the control over the systems in general, over the resources and services offered through the networks.

The cyber-attack is without borders, and ensuring the security of networks and transactions through such megacities is the biggest challenge in this area.

Cyber defence involves the protection of networks against a wide range of minor "spam" attacks, up to the major ones, such as malicious code attacks (viruses, worms), unauthorized access to the system (intrusion), blocking or destroying a service system, espionage, forgery of authenticity.

Therefore, in today's society, an indispensable objective becomes the creation of the capacity to respond to security incidents in the communications networks, meaning the implementation of a *CERT* (Computer Emergency Response Team) *capability.*

As borders do not represent a barrier to cyber-attacks, the conclusion is that the operationalization of an international CERT capability, in response to these aggressions, must be integrated into a global system. Thus, the creation of a European secure communications infrastructure is an objective mentioned in the documents of the Parliament, the Council and the EU Commission. Also, NATO has set this goal for the Alliance's cyber space. Such a secure infrastructure cannot be designed without being associated with a coherent CERT capability. Therefore, in order to finalize a global image in the field of cyber security at NATO and EU level, it is necessary for *the regional / national CERTs to have the maximum coverage, so that in their affiliation with the international CERT organizations it can have a substantial contribution.*[9]

Directions of action in the transformation of Intelligence

The evolutions of the new international context generated by the political, economic and social changes have given a strong impetus to organized crime activity, but also to terrorist actions. At present, it can be seen, from the assessments of the intelligence services, that these transnational criminal organizations threaten national sovereignty and state authority,

[8] Curculescu Gabriel, Ştefan Mircea, quoted art.., p. 98.

[9]The acronym CERT comes from the English term Computer Emergency Response Team, which can be translated into Romanian as the Cyber Emergency Response Team. A closer translation of this term is the Cyber Security Incident Response Team, which is mapped to a somewhat more commonly used abbreviation in the European space, CSIRT (Computer Security Incident Response Team). GUIDE on the role of CERT structures and the usefulness of private CERTs - https://cert.ro/vezi/document/rolul-certurilor-si-utilitatea-celor-private

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

democratic values and public institutions, national economies and have become a global threat to international security. Benefiting from the advantages of modern technology, the successes in improving weapons of mass destruction and not infrequently, the masked support of some states, *"terrorists have the ability to provoke real massacres, by means of superviolent actions, to threaten and to hold in chess even powerful states "*[10].

The existence of the mentioned types of threats requires that the information services be adapted to the new challenges, so as to provide the political and military decision-makers with the information necessary to make the decisions to counter the threats. Intelligence is needed to discover the aggressive intentions of an adversary and to define them, such as indirect aggression or preparing for the next step in intensifying the threat. In other words, effective intelligence is needed to prevent threats.

The new threat configuration has led the countries in the Euro-Atlantic area to carry out major reforms, materialized through strategies, security policies, action plans and regulations. Under these conditions, one of the directions of action in the transformation of the information services has materialized in the efforts of the states to improve and expand the legal framework for the organization and operation of the information services and to ensure their financial support for a more efficient functioning. At the macro level, the efficiency of the transformation process implies the establishment of three sets of objectives: the efficiency of the institutional management, the increase of the operational capabilities and the consolidation of the capacities of analysis, planning and evaluation in the intelligence activity.

Depending on the new threat configuration, the intelligence services' efforts to streamline and adapt their structures, methods and means have resulted in transformative directions such as reorganizing and coordinating information communities. Another important direction is aimed at developing the technical capabilities for collecting information by updating the means and methods of data collection, as well as the techniques of operating with the equipment owned by intelligence services. At the same time, emphasis is placed on obtaining information from human sources. Beneficiaries / decision-makers need, more than ever, access to the subtle mechanisms of international politics, respectively, to know the beliefs, thought processes, intentions, vulnerabilities of political opponents, and these data are more complete and nuanced collected from human sources; the fact that in the war on drugs and terrorism, espionage technology is not yet adequate enough has revived interest in HUMINT; the human element has proved decisive for the operation of any information service, both in the field of information and special operations, with incomparably lower costs than those allocated to electronic means.

Another dimension of the transformation of intelligence services is represented by the trinome cooperation - cooperation - collaboration, which expresses concrete ways by which intelligence services act in order to achieve common objectives by concluding bilateral and multilateral agreements, elaborating regional and international instruments that foresee effective, immediate and forward-looking measures to combat global threats.

Perspectives

The unpredictable, highly fluid and dynamic international security environment, characterized by complexity, represents the image of the overall evolution of the political and economic framework of the last decades. In this environment, current and future challenges will permanently influence and change the geopolitical context that intelligence professionals are currently analysing.

[10] Anghel Andreescu, Niţă Dan, Terrorism. Psychological analysis, Tripolis Publishing House, Timişoara, 1999.

Technium Social Sciences Journal
Vol. 8, 737-744, June 2020
ISSN: 2668-7798
www.techniumscience.com

With all the impressive discoveries in sensors, automation, technical collection and decoding, the role of HUMINT and analysts remains important in providing high-performance intelligence. There is simply no substitute for efficient managers, accurate analysts, capable linguists and dedicated spies.[11]

Effective intelligence is needed to prevent threats. Cooperation in the field of intelligence imposes a new stage in the co-operation between the information services: the shift of the centre of gravity from the exchange of information of generality character to the cooperation on cases and punctual actions, as a way to optimize the potential offered by the partners involved.

References

[1] Anghel Andreescu, Niţă Dan, *Terrorism. Psychological analysis*, Tripolis House Publishing, Timişoara, 1999.
[2] Bergesen J. Albert, Omar Lizardo, *International Terrorism and the World-System. Compendium of Counterintelligence Training and Education* (Private/Academic Course Offerings) the National Counterintelligence Institute Office of the National Counterintelligence Executive March 2007.
[3] Curculescu Gabriel, Ştefan Mircea, *Cyber aggression in the Euro-Atlantic area*, Intelligence Magazine no. 25 of September 2013.
[4] David A. Clark, *The Elgar companion to development studies*, Edward Elgar Publishing Limited Publishing House, UK, 2006, p.200.
[5] Dupont, Alan, *Intelligence for the twenty-first century*, in Intelligence and National Security, no.4/2003.
[6] Ionel Bucuroiu, *Information services in the 21st century and security issues* in Pulsul geostrategic, no. 30, June 2008, Braşov.
[7] Joshua s. Goldstein, John C. Pevehouse, *International Relations*, Polirom Publishing House, Iaşi, 2008, p. 400.
[8] Lahneman, William J., „*Is a Revolution in Intelligence occurring?*", in International Journal of Intelligence and Counterintelligence, 20, 1-17, 2007.
[9] Maior, George, *The new ally: rethinking Romania's defence policy at the beginning of the 21st century*, Rao Pulishing House, Bucharest, 2008.
[10] Matei, Mihaela, The transformation of the intelligence systems and the modernization process of the Romanian Intelligence Service, Intelligence Magazine no. 25, September 2013.
[11] Tiberiu TĂNASE, Roxana TUDORANCEA Transforming intelligence in the context of the new challenges of the 21st century, p 149, *Revista Română de Intelligence* No. 1-2/ 2009.
[12] Tanase, Tiberiu, US Defence Intelligence - the community and the Department of Defence intelligence strategy, Gândirea Militară Românească no. 2/2010, March - April 2010.
[13] Tanase, Tiberiu, *Security and Intelligence Strategies for the 21st Century*, the XVII - Session of Scientific Communications, National Academy of Information, November 22, 2011.
[14] Tanase. Tiberiu, Considerations *regarding the impact of global threats on Intelligence communities. The importance of modelling them through new security and intelligence strategies* ANI Bucureşti Publishing House, November 12, 2010, 16th Session of

[11] Infosfera no. 4 /2018 https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2018/4_2018.pdf

Scientific Communications with International Participation of the National Academy of Information "Mihai Viteazul.

[15] Tanase Tiberiu, *Views on the Department and Strategies on Homeland Security and Intelligence,* Universitătii Lucian Blaga Sibiu Publishing House, 2010.

[16] Tanase Tiberiu, *Cooperation in the field of intelligence in the European and Euro-Atlantic area,* National Defence University, UNAP Publishing House, 2010.

[17] Adrian Robu The image of the threat. Sensors, Sources of Knowledge - Intelligence Magazine, March 30, 2020 https://intelligence.sri.ro/imaginea-amenintarii-senzorii-surse-ale-cunoasterii/

[18] Satellites *Defence Support Program (DSP)* http://www.esri.ro/industries/defense/arcgis-for-intelligence