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.

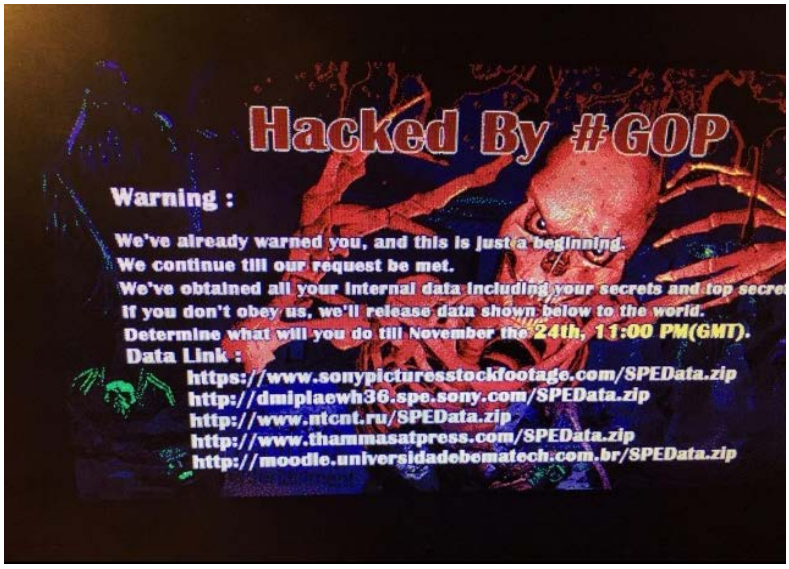

Figure nr. 1 – The message received by Sony Pictures' employees on 24.11.2014
Source: https://pmcdeadline2.files.wordpress.com/2014/11/hacked-by-gop-sony-pictures-under-attack.png?w=970

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 puțin probabilului*, Bucureşti: Editura Curtea Veche.