„CAROL I" NATIONAL DEFENCE UNIVERSITY
Centre for Defence and Security Strategic Studies

P R O C E E D I N G S

INTERNATIONAL SCIENTIFIC CONFERENCE
STRATEGIES XXI

THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT

Volume 2

Editors
Stan ANTON
Iuliana SimonaȚUȚUIANU

June 11-12, 2015
Bucharest - Romania

INTERNATIONAL SCIENTIFIC COMMITTEE

Gabriel - Florin MOISESCU, PhD., professor, "Carol I" National Defence University, Romania
Ion ROCEANU, PhD., professor, "Carol I" National Defence University, Romania
Gheorghe CALOPĂREANU, PhD., professor, "Carol I" National Defence University, Romania
Stan ANTON, PhD, lecturer, "Carol I" National Defence University, Romania
Bogdan AURESCU, PhD., assoc. professor, University of Bucharest, Romania
Silviu NEGUȚ, PhD., prof., Bucharest Academy of Economic Studies, Romania
Péter TÁLAS, PhD., Center for Strategic and Defense Studies, Hungary
Iulian CHIFU, PhD., assoc.professor, National School for Political Science and Public Administration, Romania
Piotr GAWLICZEK, PhD., assoc.professor, National Defence University, Poland
Sorin IVAN, PhD., prof., "Titu Maiorescu" University, Romania
Rudolf URBAN, PhD., professor, Defence University, Czech Republic
Pavel NECAS, PhD., professor, dipl. eng., Armed Forces Academy, Slovakia
Stanislaw ZAJAS, PhD., professor, National Defence University, Poland
Ilias ILIOPOULOS, PhD., professor, Hellenic, Naval WAR College, Greece
Georgi DIMOV, PhD., assoc. prof., "G. S. Rakovski" National Defense Academy, Bulgaria
Ioan CRĂCIUN, PhD., professor, "Carol I" National Defence University, Romania
Daniel FIOTT, Fellow of the Research Foundation - Flanders, Belgium
Florin DIACONU, PhD., assoc. Professor, Bucharest University, Romania
Nicolae RADU, PhD., professor, "AlexandruIoanCuza" Police Academy, România
Marius-Cristian NEACȘU, PhD., assoc. prof. Bucharest Academy of Economic Studies, Romania
Silviu PETRE, PhD., Center for East-European and Asian Studies, Romania
Bogdan SAVU, PhD., Military Medical Institute, Romania
Pascu FURNICĂ, PhD., "Carol I" National Defence University, Romania
Ciprian PRIPOAE, psychologist, National Defence University, Romania
IulianaSimona ȚUȚUIANU, PhD., senior researcher, "Carol I" National Defence University, Romania
Cristian BĂHNĂREANU, PhD., senior researcher "Carol I" National Defence University, Romania
Mirela ATANASIU, PhD., researcher, "Carol I" National Defence University, Romania
Cristina BOGZEANU, PhD., researcher, "Carol I" National Defence University, Romania

Scientific Secretary:
Alexandra SARCINSCHI, researcher PhD., "Carol I" National Defence University, Romania

ORGANIZING COMMITTEE
Stan ANTON, PhD, lecturer.
Irina TĂTARU, PhD.
Daniela RĂPAN
Doina MIHAI
Ionel RUGINĂ

PRODUCTION EDITORS:
Elena PLEȘANU
Daniela RĂPAN
Doina MIHAI
Irina TĂTARU

COPYRIGHT: Ani reproduction is authorized, without fees, provided that the source is mentioned.
Authors are fully responsible for their papers content

ISSN 2285-9896
ISSN-L 2285-8318

EXPERIMENTAL RESEARCH OF PSYCHO - INFORMATIONAL DISTAL INFLUENCE[1]

Aliodor MANOLEA, PhD
Doctor of Psychology (Ph.D.), University of Bucharest
Doctor of Science - Complementary Medicine (D.Sc.), The Open University for the Complementary Medicines, Colombo, SriLanka.
Ph.D. Candidate in Military Science, "CAROL I" National Defence University, Bucharest.
e-mail: aliodor@glide.ro

Abstract: *The experimental demonstration of the transmission of information, apparently without material support, in warfare operations, is possible by recording the EEG pattern of brain activity produced by exposure to the emotional visual stimuli between spatially and sensory isolated subjects. The phenomenon of brain connectivity, during what we called Distant Psycho -Informational Influence, is demonstrated by determining of the coherence of the signals and using the ERD / ERS neuroscientific classifier.*

Keywords: *psycho-informational, distal, subliminal, coherence, synchronization*.

The phrase Distal Psycho-informational Influence (IPsiD) is an integrating concept, which includes an extension of subliminal communication and influence in the kinetic domain of action[2]. The purpose of using distal psycho-informational influence, in all the steps of the warfare action, is to alter the psycho-emotional capacities of the enemy need to carry out combat operations, to diminish their capabilities to make decisions, at all levels, from the commanders to the troops, to weaken the enemy's determination to fight.

Structure of the Experiment

The experiment consisted in the simultaneous exposure of inductor subjects to visual stimuli with emotional signification and in measuring the effect of the supposed distal psycho-informational transmission to receptor subjects. The brain activity of both categories of subjects was monitored using wireless one-channel MindWave Mobile EEG headsets, which were conected with a data-acquisition system including three laptops, with time synchronizing covered through the internet. The operating system used was LINUX. The electrode of each EEG headset was placed in the prefrontal lobe area of each subject, in the Fp1 point in the placing scheme 10-20 of the EEG electrodes on the scalp. The master computer was running the PSYCHOPY[3] application, which managed the temporal unfolding of the experiment, concerning the exposure to visual stimuli with emotional contents. Visual stimuli were displayed simultaneously for all inducer subjects on displays M1...M8 by means

[1]A., Manolea, *Acţiunea beligenă şi influenţarea psihoinformaţională distală,* referat Scoala Doctorală Ştiinţe Militare şi Informaţii, UNAp, Bucureşti, pp.4-65.
[2]A., Manolea, *Influenţa psihoinformaţională distală ca parte a influenţei informaţionale de intelligence*. Academia Nationala de Informatii "Mihai Viteazul" International conference „Intelligence in the knowledge society" Bucharest, Romania, October 19th, 2012. Biblioteca electronica a Academiei Nationale de Informații (ANI), Colectia "ANI - Mihai Viteazul", ISBN 978-606-532-062-3.
[3]J.W., Peirce, *Generating stimuli for neuroscience using PsychoPy*. Frontiers in Neuroinform. 2:10. doi:10.3389/neuro. 11.010.2008.

of a video distributor (VS). On the appropriate displays, receptor subjects could see only black mark on the center of the screen.

Three experiments were carried out, unintentional and intentional, each on 16 inexperienced subjects (without specific psycho-informational training) and another intentional one on 16 subjects, of which eight subjects had particular psycho-informational training (activation of own potential by the neutral technique). On the whole there were 48 subjects participating to these experiments, of which 40 were students of the Faculty of Psychology of the Bucharest University and eight belonged to a group with specific psycho-informational training.

All three experiments were carried out during the same temporal timeframe. Each test included 25 sessions to which participated groups of subjects distributed using the Fibonacci sequence[4].

Each session of each trial included nine images, each with a duration of six seconds, preceded by a warning pause of 4 seconds, some with positive emotional contents, other with negative contents and other emotionally neutral.

The uneven number sessions (1, 3, 5... 25) had as inductors subjects from Room 1, and for the even number ones inductor subjects from Room 2. There were eight subjects in Room 1 and eight in Room 2, isolated spatially by a reinforced concrete wall.

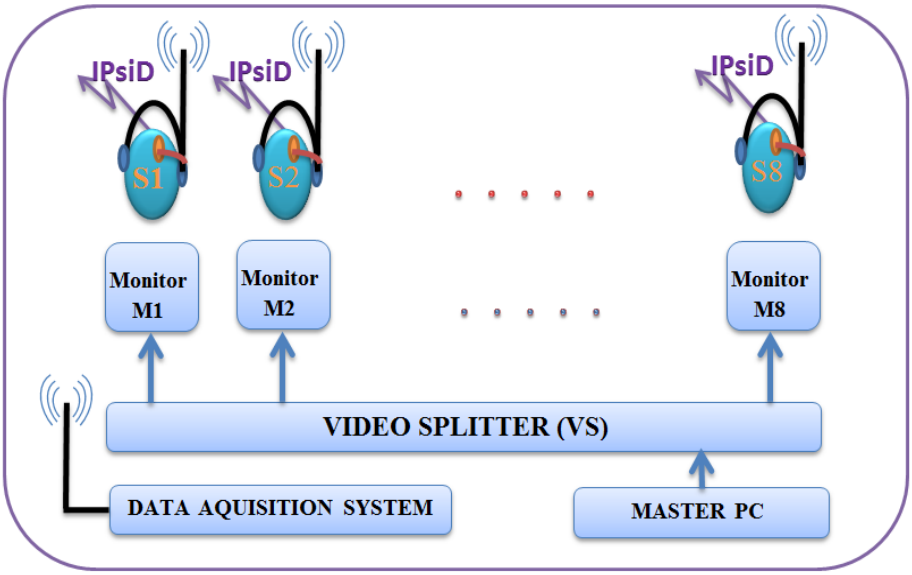

Figure no. 1 Experimental mounting for subjects in Room 1 (Manolea, A. 2014)

There were measured, synchronized in time, the brain activity of the inductor and receiver subjects, and have processed the obtained data using several application packages for the signals analysis: EXCEL, MATLAB, EEGLAB and ASAEEG, in order to extract the information packed in the EEG structure. All individual EEG channels have been reunited in a structure corresponding to the EEG 10-20 scheme, with a maximum of 19 channels, out of which only 15 channels were activated, because one channel of the data acquisition system did not work.

The EEG recording corresponding to each subject was assimilated to one channel, specific for the recording of one EEG with the 10-20 electrodes system.

[4] A., Manolea, *Fundamente epistemice ale influenţei psihoinformaţionale distale,* Buletinul UNAP nr.1/2013, pp. 378-382.

The correspondence was: S1-Fp1, S2-Fp2, S3-F7, S4-Fz, S5-F8, S6-T3, S7-Cz, S8-T4, S9-O1, S10-O2, S11-T5, S12-P3, S13-Pz, S14-P4, S15-T6 and S16-Oz, where S_i are the 16 subjects. In so doing, were able to use the analytical facilities of the EEG analysis program, which simultaneously process all the signals, so that the results were obtained in a unitary manner, by using the same processing procedures, with the same values for the specific parameters.

Thus, EEG electrodes corresponding to the front half of the model scalp corresponded with the EEG recordings of subjects in Room 1 and the ones of the back of the head corresponded to the EEG recordings of subjects in Room 2.

Methods for Studying the Synchronization of Brain Activity

The hypothesis behind any EEG analysis is that the certain patterns of brain activity always correspond to the same triggering events and the other way round, in other words that there is a bi-univocal relation between triggering events and the pattern of brain activity. In our case, the triggering events were the emotions generated by the exposure of inductor subjects to images with emotional contents, and the assumption was that by some mechanism, so far unexplained, these emotions are distally sent to other subjects, without them being in any whatsoever contact and without any awareness[5]. In fact the intention was to measure what happens, how and whether any information is sent from the inductor subjects to the receiver ones, when the intention is present and when it is not. At the data processing level, this fact is equivalent to the existence of common patterns of brain activity, both of inductor and receptor subjects.

This analysis is based on the supposition that brain activity is specific to each interaction of the human being with the environment, whatever it may be, or, in other words, adapted to our case, each emotion produces a particular pattern of brain activity. If we find similar structures in the time or frequency domains then we can say that there is a high degree of similarity between the events (emotions) that have caused that structure of brain activity in inductor subjects.

ERS/ERD–Event Related Synchronization/Event Related Desynchronization Method

A typical method to analyze EEG is the averaging of data in order to identify certain structures, patterns appearing at certain fixed moments in time, related to specific events (e.g. stimuli or responses to stimuli) – the so-called ERP's (Event Related Potential). By averaging, the signal-noise ratio is dramatically improved so that a certain characteristic structure becomes visible. However, in many cases (such as the present one), there are no well determined moments in time, related to the appearance of brain activity related to a certain event, because we do not know how and when an image with emotional contents causes an emotion in the mind of the inductor subject. The electrical activity of the brain of the inductor subject, produced by emotions, can be caused by his/her memories or some unconscious mechanism related to instinctive reactions like fight or flight, so there is a non-determination regarding the moment of arising of a pattern of the electrical activity of the brain (EEG).

The non-determination, about the moment of occurrence of the transmission of information, is specific for the distal psycho-informational influence (IPsiD). So if we use the

[5] [5]A., Manolea, *Fundamente epistemice ale influenţei psihoinformaţionale distale,* Buletinul UNAP nr.1/2013, pp. 378-382.

ERP determination method, the information will be destroyed by the averaging because it does not appear at the same intervals from the triggering event for all the sessions of the experiment. This fact can be avoided by applying the method of synchronization / desynchronization analysis (ERS / ERD – Event Related Synchronization / Event Related Desynchronization) to the brain activity determined by the occurrence of certain events at somehow random moments in time. ERS represents an increase in amplitude of the power of brain waves in a particular band of frequencies, of short duration and well localized spatially, whereas ERD represents a decrease of amplitude. These increases /decreases in amplitude are not correlated in phase with a certain event and are very specific for certain bands of frequency (alpha, beta, gamma, delta and theta), i.e. they can appear in certain bands of frequency but not in others. For this reason, the unprocessed EEG recordings look like a chaotic, random signal, which does not seem to contain very clear patterns of brain activity, unless in well known cases.

The calculation of ERS and ERD is used to get an image of the dynamics of neural networks, in our case of the dynamics of links between the brain activities of inductor and receptor subjects.

EEG Coherence Method

Another method used to show there is a similarity between two EEG signals is the calculation of the coherence between them. The coherence is similar to the temporal correlation between two signals, but it is an estimator of similarity (giving us an image of the coupling of signals) in the frequency range. Coherence can show us there are common patterns of brain activity in certain frequency bands, whereas the temporal correlation is masking these patterns. Coherence is a complex function, of which the amplitude varied between 0 and 1. Here zero shows a lack of similarity between signals and values close to 1 a high similarity.

Preliminary Results

We must not forget that the image of brain activity as shown here is a simulation of the brain activity of all the subjects in the experiment, each EEG signal corresponding to one subject. Thus, an image of the standard scalp contains up to 15 virtual electrodes corresponding to each subject. In the case of the uneven number sessions of the experiment, the group of electrodes Fp1, Fp2, F7, Fz, F8, T3, Cz and T4 represent inductor subjects, and the group of electrodes O1, O2, T5, P3, Pz, P4 and T6 receptor subjects, the roles being reversed for sessions with even number.

Testing of Hypothesis

Hypothesis no.1 *Highlighting the existence of temporal synchronization of brain activity models (patterns) common both to inductor and receptor subjects.*

The results presented further have been obtained using the application package for the interpretation of EEG records, EEGLAB[6], a project coordinated by Swartz Center for Computational Neuroscience (SCCN) of the Institute for Neural Computation of the University of California, San Diego.

In the figure no. 2 we note the variance of intensity of the connection between brain activities of two subjects during an experimental distal influencing session. The highest EEG

[6] A. Delorme, S. Makeig, „EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics". *Journal of Neuroscience Methods* 134:9-21, 2004.

power, common to both subjects, is in the delta and theta (1-7,5Hz) frequency domain of brain waves. The theta frequency range characterizes the subconscious activity, the domain of subliminal perceptions.

Also, we note the rhythmic variation of the intensity of connection of brain activities of both subjects. A curve which shows for the most part a strong correlation (the maximums of the graph are in the intervals 10-20s, 30-40s, 60-70s, 70-80s, 80-90s) to the moment when images with emotional contents appear. Images with an emotional effect have appeared at 14s, 24s, 34s...94s, i.e. intervals of ten seconds, with the duration of six seconds. This fact was recorded in most of the experimental sessions with higher or lower frequency, depending on four factors. The first factor was the ability to focus and keep it for a sufficiently long time, to enable us to say that the power of brainwaves was sufficiently high to generate such effects. The second factor is related to the concentrated focus which a subject can show, a factor with a high variability especially when it has to be maintained for a long time, in our case nearly 100 seconds. In general, an untrained subject cannot keep his/her attention focused on only one mental objective for more than a few seconds. The third factor is the training that the participating subjects have undergone. Of the 48 participating subjects, only eight have had a specific training for the improvement of their capacity to maintain attention and focus, the others being classified in the normality profile. The fourth factor was the activation of the own potential using the neutral technique, an activation which is part of the training program, of which the same eight subjects have benefited.

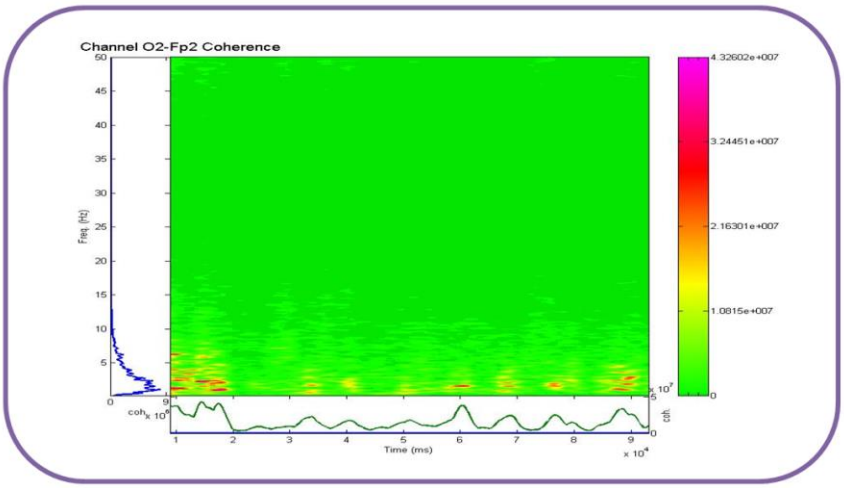

Figure no. 2 Interaction between the brain activities of two subjects (S2 and S10) represented in the frequency domain (left graph) from and in the time domain (lower graph). The graph in the center shows the connection of the two subjects both in frequency and in time (Manolea, A. 2014)

Also, if we study the connection between the subjects by using the method of ERS/ERD assessment (figure no. 3) we note, this time on a global scale (for all the subjects at once), how alternations occur between the coupling (ERS synchronization) and decoupling moments (ERD desynchronization).

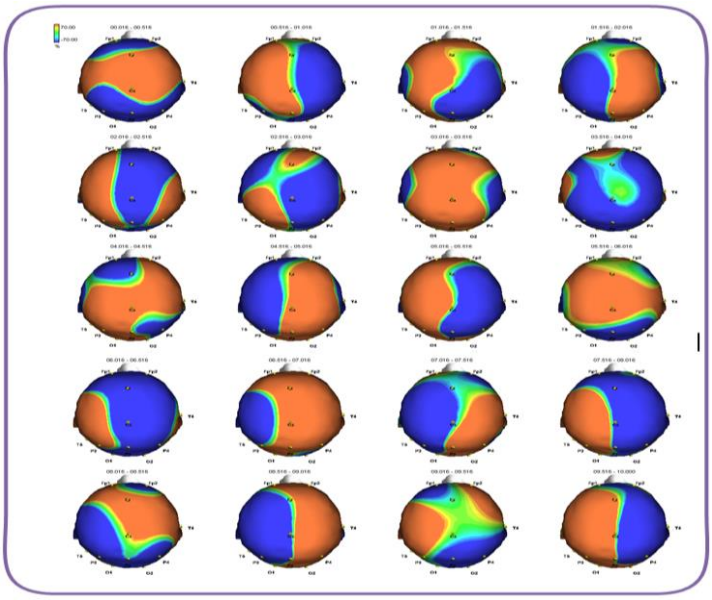

Figure no. 3 Dynamics of ERD/ERS (synchronization - desynchronization of brain activity) in the interval of 10-20 seconds (every 0.5 s) of the experimental session and the theta range (2-4 Hz). The synchronization of the brain activity is rendered in red and the desynchronization in blue EEG electrodes positioning on the scalp, according to system 10-20 (Manolea, A. 2014)

The moments of synchronization correspond to an increase in power of brain waves, and the desynchronization ones to a decrease of this power[7]. We also note how various subjects become connected (synchronized) on turns or together, this being a feature highlighted by this type of analysis[8]. Thus, we can say that the subject can be related to more subjects. We note there are short intervals (less than 0.5 seconds) when the brain activity of the involved subjects takes a break, becomes desynchronized, detached. The neural networks of the receptor subject show a maximum of availability[9] to the distal influence.

Therefore, the influencing action seems to occur in impulses. In fact that a higher power can be available only for short periods of time, among others also due to the possibility of subjects to maintain their attention and focus fixed for a longer or shorter interval.

We can thus say that there is rhythmic temporal relationship between the patterns of brain activity of the subjects participating to this experiment.

Hypothesis no.2 *The subjects whose own power was activated were less influenced than the ones who did not go through such a process.*

Another modality to show the connectivity between two systems is to highlight the coherent function. This function serves to estimate the correlation between two systems in the frequency domain. Images shown further indicate the amplitude of coherence between all the 15 subjects participating to the two experimental sessions of the type eight inductors and seven receptors, changing roles on turn.

[7] Durka, P. J., Zygierewicz, J., Klekowicz, H., Ginter, J., Blinowska, K. J."On the statistical significance of event-related EEG desynchronization and synchronization in the time-frequency plane". *Biomedical Engineering, IEEE Transactions*, 51(7), 2004, pp.1167-1175.

[8] O., Brazdău, „Constiinta si misterele fizicii cuantice", *Buletinul psihologiei transpersonale*, Numărul 7-8/2003, http://www.arpt.ro/RO/TPBuletin/7-8-2003.htm, accesat 11.11.2012.

[9] G., Pfurtscheller, F.H., Lopes da Silva „Event-related EEG/MEG synchronization and desynchronization: basic principles". *Clinical neurophysiology*, Vol. 110, No. 11. (November 1999), pp. 1842-1857.

Commission, 2012[12] document by which every European citizen who feels offended by online material related to his person, may request withdrawal them. But more important than that is the "EU Code of rights in the online environment" in which Section 1, Chapter 4 (1), provides: "Every individual has the right to adequate protection of their personal data.[13]"And also paragraph 2: "Individuals are entitled to receive from individuals and businesses that have some of their personal data in the obvious such as websites, databases, service providers, etc., and correct or delete such data if it is incomplete or inaccurate[14]. Therefore secret services of the Member States play an essential role in maintaining a balance between the rights of citizens and maintaining national security and protect government interests[15]. Threats are more numerous every day, therefore aims to develop a system and how best to meet the needs for national and individual.

In addition to the general vision of online rights infringements by national authorities want to raise the issue hackers pose a threat to personal information and financial ones. Only in 2014 one of the most representative virus threat was "Heartbleed" known to enter social sites such as Facebook, Instagram, Pinterest, Tumblr, Google and Yahoo[16]. The recommendation of these companies after the attack was to change our passwords. They also took the initiative to form a joint program of defense against future threats, each allocating an amount of $ 100,000 annually[17].

The result of research analyzing the above events has reached three distinct results that will fit in states where national policy towards freedom that the Internet offers: free internet, semi-free internet and censored. I wish to make an observation on the first category, free internet, not only is guaranteed by law, but it also actively promotes this idea. Talking further about the semi-open Internet, where the government intervenes and oversees its citizen's intense activity in defiance of human rights. With limited freedom and censor the Internet, defines national policy authoritarian states characterized by control of access to the Internet, where online privacy rights there. I placed at the top of the Internet free EU states, also United States we have cataloged in the second category of semi-free Internet and China belongs to the third category of Internet censorship.

2. The Cyber War

The term "cyber war" could not be provided with a concrete definition, being very controversial in the international community. The main resource of this war is the information itself and its damage by careful speculation obtained vary, handling and pushing people to revolt to millions of dollars in damages. In this chapter I want to remember the concepts of "cyber espionage" and "cyber terrorism". We define the term cyber espionage fraudulently entering into private or government information bases and their transfer without consent of the owner. The second concept relates to cyber terrorism attacks on hardware devices and software via the Internet aimed at causing irreparable damage.

---

[12] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Factsheet data protection, accessed on: 21.03.2015

[13] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20RO%20final.pdf, Code EU online rights, accessed on: 24.04.2015

[14] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20RO%20final.pdf, Codul UE al drepturilor in mediul online, accessed on: 24.04.2015

[15] Tom DYSON, Theodore KONSTADINIDES, *Europe Defense Cooperation in EU law and IR theory*, Palgrave Macmillan, Hampshire, 2013, p. 19

[16] Office of the Privacy Commissioner of Canada, *Privacy and Cybersecurity: Emphasizing privacy protection in cyber security activities*, 2015, p. 1

[17] http://mashable.com/2014/04/24/facebook-google-microsoft-join-forces-to-prevent-another-heartbleed/, Facebook, Google, Microsoft Join Forces to Prevent Another Heartbleed, accessed on: 23.04.2015

Next we examine changes in bilateral and multilateral relations between states as a result of increased cyber warfare. Since 27 April 2007, when Russia attacked the official websites of Estonia, causing great damage to the government in Tallinn, demonstrating the existence of a new weapons NATO forces in international relations[18]. Also worth mentioning is the Russian-Georgian war, when Russia attacked Georgia all sites showing her inability cyber defense. Every country in the world their own arrangements for the preparation of a cyber defense which match the internal political environment. Among the most relevant examples of this is the UK, announcing publicly that threats via the Internet are real ones. A measure taken by the Conservative government is launching a campaign to recruit IT experts to create a team to combat the threats initiated by the Ministry of Defence[19]. Latvia is another European who noted that virtual environment security is very important, which is why he began recruiting a team to counter international threats[20]. Experts explain that unlike a real opponent, the opponent can come online from anywhere in the world, even within the state from a state allied or enemy. Austria, the first state is not a NATO member, decided to join the Alliance Center of Excellence of cybersecurity[21]. Ministry of Defence of Japan took the initiative establishment of a team of about 90 people, as the unit of cybersecurity to protect national interests in the virtual environment[22]. Under Obama, the US cyber defense budget increased over time, wanting a greater focus on combating attacks faced by the country.

Current international situation proves one thing: the trend of multipolarity, unlike the last century, where the world was divided into spheres of influence bipolar. As we can see, is approached a different perspective, but they all share one thing: fighting threats by the Government through specialized recruitment of a new kind of war. Multilateral treaties based on compromises the potential to give rise to effective cyber security projects, as I mentioned above about Alliance Center of Excellence of cybersecurity.

Financial Report of the World Economic Forum in 2014 clearly demonstrates and gives a warning on the issue of effective cyber defense system effectively bring international loss of around 3 billion by 2020[23]. Descendants of increasingly large data obtained digitally converts them into vital targets for attackers who want to interfere with governmental and international systems. From this we can deduce that the targets by aggressors since they have a weaker defense system, the more easily attacked. As James B. Comey also mentions in his speech at the International Conference on cyberdefence Forham University of New York, 2015: "Our life has changed thanks to the Internet, and everything is a threat evolved.[24]"

The consequences of inefficient state cyber defense system: closing sites, information theft, espionage, but I will focus on the most relevant. Among the many threats facing citizens and public institutions on the Internet every day, we remembered viruses and best known of these is Stuxnet, preconceived to destroy industrial systems. Its presence was confirmed both in the US, Europe and Asia, in Iran attacking a nuclear systems, causing huge

[18] http://www.theguardian.com/world/2007/may/17/topstories3.russia, Russia accused of unleashing cyberwar to disable Estonia, accessed on: 21.03.2015

[19] http://www.bbc.com/news/uk-24321717, UK creates a new cyber defense force, accessed on: 21.03.2015

[20] http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936, Latvia launches cyber defense unit to beef up online security, accessed on: 21.03.2015

[21] http://www.defensenews.com/article/20140512/DEFREG01/305120014/Austria-First-non-NATO-Nation-Join-Alliance-Cyber-Defence-Centre-Excellence, Austria first non-NATO nation join Alliance cyber defense center, accessed on: 21.03.2015

[22] http://www.janes.com/article/35956/japan-establishes-cyber-defence-unit, Japan establishes cyber defense unit, accessed on: 21.03.2015

[23] World Economic Forum, *Risk and responsibility in a Hyperconnected world*, 2014

[24] http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, International Conference on Cyber Security, Fordham University, accessed on: 23.04.2015

damage[25]. The second case is the Russian virus Rocra, who for years has stolen government information from countries that have not detected[26]. Daily notifications on threats in this area, data are available in the report of the Strategic and International Studies Center, aiming at online crime carefully[27]. We see from these examples of what is needed and priority adaptation cyber defense strategy.

Individualistic tendency of states to the problem of cyber conflict demonstrates the method of compromise between national public and private sphere to achieve the best results in terms of security. Note also the diplomacy between states, we can see that they confirm the theory of realism in international relations, where states act in order to achieve their interests. Vulnerabilities of a defense systems compromise the information in heritage and further damage resulting is huge. Threats are becoming more numerous every day, therefore the budget allocated by the states to improve cybersecurity is increasing from year to year in direct proportion to the threats they face.

Conclusions

I followed closely the effects of involvement of the individual in political life and notice the changes it brought in a short time in a field so new. We went through two chapters of research seeking answers to the question: "How can we combat cyber terrorism and at the same time respect for privacy and freedom of individuals in an online environment, given that accredited institutions may be abuse of this information?". I noticed that each state has adapted its own policy on the subject under discussion and the methods are determined by history and international experiences. While Russia prefers a more aggressive approach on cyber security, China seeks to impose censorship to control the interior and exterior threatening. The United States of America has an intrusive approach in people's lives, in order to have an efficient cybernetic system. Instead member states of the European Union took a different approach on the situation choosing a balanced way, seeking to satisfy both sides.

The United Nations plays an important role in defining the future of bilateral relations and respect for individual rights via the Internet initiative. However it is not sufficient, it is necessary involvement of powerful states and other international organizations. From studying primary bibliography consists of: treaties, legislation and interviews, we answer the question of research concluding that meets both criteria EU countries such as cyber security and rights online. If it says my research hypothesis by demonstrating the existence of an area of compromise, simple and effective. After research results in Chapter 1 we categorized states according to civil rights on the internet, the European Union entered into the first category, free internet, US Internet semi-free ranging and China as part of the third category of internet censorship . The cooperation of states and international organizations to develop the strategy limited, but it is interesting to watch now[28]. And the reason I say this is the real possibility of a war through the Internet is a threat that must be taken into account. Another perspective on this domain confers international organizations of human rights, which repeatedly criticized virtual espionage[29]. This subject can be interpreted in several ways

[25] http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, Stuxnet was far more dangerous than previous thought, accessed on: 21.03.2015

[26] http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html, Red October malware discovered after years of stealing data in the wild, accessed on: 21.03.2015

[27] http://csis.org/program/significant-cyber-events, Significant Cyber Events, accessed on: 23.04.2015

[28] Daniel VENTRE, *Cyber Conflict: competing national perspectives*, ISTE Ltd, London, 2012 , p. 182.

[29] Tom DYSON, Theodore KONSTADINIDES, *Europe Defence Cooperation in EU law and IR thory*, Palgrave Macmillan, Hampshire, 2013, p. 19.

depending on international political actor and interests. The realism theory is confirmed by research carried out in Chapter 2, from which we deduce the need to adapt to current changes in actions to increase security at the expense of international ideals. However, it is necessary to adapt our society given the changes that occur to counter emerging threats and we follow our interests while we enjoy the protection of the rights not abuse this freedom[30].

Cyber security represents a new world to explore for us having different possibilities that a few years ago seemed impossible to create. It is necessary to study the area discussed, as it has a direct impact on us, the way we get information, how we learn, how to communicate, etc. New methods are being developed every day by international political actors in order to obtain an advantage over competitors. The information in this case is essential, and also written articles and conferences on the subject should be a top priority.

BIBLIOGRAPHY:

1. ANDRESS, Janson, Steve WINTERFELD, *Cyber warfare: Techniques, Tactics and tools for security practitioners*, SYNGRESS, 2013
2. BAYLON Caroline, *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Chatham House, 2014
3. CAVELTY, Myriam Dunn, *Cyber-Security and threat politics: US efforts to secure the information age*, Routledge, New York, 2008
4. DEIBERT, Ronald, *Access controlled: The shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, Massachusetts, 2010
5. DYSON Tom, Theodore KONSTADINIDES, *Europe Defense Cooperation in EU law and IR theory*, Palgrave Macmillan, Hampshire, 2013
6. European Commission, Factsheet on the "Right to be forgotten" ruling (c-131/12), Bruxelles, 2012
7. KARATZOGIANNI, Athina, *Cyber conflict and global politics*, Routledge, New York, 2008
8. KLIMBURG, Alexander, *Naţional Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012
9. NORRIS Pippa, *Public Santinel: News Media & Government reform*, The World Bank, Washingston, 2010
10. Office of the Privacy Commissioner of Canada, *Privacy and Cybersecurity: Emphasizing privacy protection in cyber security activities*, 2015
11. SHACKELFORD, Scott J, *Managing Cyber Attacks in International Law, Business, and Relations: In search for cyber peace*, Cambridge University Press, Cambridge, 2014
12. VENTRE Daniel, Cyber Conflict: competing national perspectives, ISTE Ltd, London, 2012
13. World Economic Forum, Risk and responsibility in a Hyperconnected world, 2014
14. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/17/27, 2011
15. https://freedomhouse.org/country/china#.VIiPmXuPVoM, Freedom House China

[30] Myriam Dunn CAVELTY, *Cyber-Security and threat politics: US efforts to secure the information age*, Routledge, New York, 2008, p. 27.

16. http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?_r=0, China toughens restrictions on internet use
17. http://www.huffingtonpost.com/2012/02/29/china-firewall-breach_n_1308836.html?, China firewall breach
18. https://freedomhouse.org/country/united-states#.VRaVH-G1doM, Freedomhouse SUA
19. http://www.spiegel.de/international/topic/nsa_spying_scandal/, NSA spying scandal
20. http://www.theguardian.com/world/2007/may/17/topstories3.russia, Russia accused of unleashing cyberwar to disable Estonia
21. http://www.bbc.com/news/uk-24321717, UK creates a new cyber defense force
22. http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936, Latvia launches cyber defense unit to beef up online security
23. http://www.defensenews.com/article/20140512/DEFREG01/305120014/Austria-First-non-NATO-Nation-Join-Alliance-Cyber-Defence-Centre-Excellence, Austria first non-NATO nation join Alliance cyber defense center
24. http://www.janes.com/article/35956/japan-establishes-cyber-defence-unit, Japan establishes cyber defense unit
25. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, Stuxnet was far more dangerous than previous thought
26. http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, International Conference on Cyber Security, Fordham University
27. http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html, Red October malware discovered after years of stealing data in the wild
28. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Factsheet data protection