DEFINING CYBERSECURITY AS THE SECURITY ISSUE OF THE TWENTY FIRST CENTURY. A CONSTRUCTIVIST APPROACH

Ionela Maria CIOLAN
National University of Political and Administrative Sciences, Bucharest
Tel: 004-0318.08.97, E-mail:ciolan.ionela@gmail.com

"The cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century." (Nye, 2010, 19)

Abstract
Nowadays, ICT play an important role in our lives: from entertainment purposes to communication and information activities to conducting a business or taking advantages of the digital public services. Human dependency upon digital space is also present in governmental and international activities and it is on an increasing trend. Nevertheless, the usage of new technologies doesn't offer us only benefits, it also comes with great cost. Cyberspace due to its fast, cheap and anonymous characteristics has became a place for different sort of cybercrimes and attacks. In this condition, the protection of cyberspace and the creation of an efficient and clear cybersecurity policy are among the most important issues on the national and international security agendas. Therefore, this paper aims to analyze the current situation and debates regarding cybersecurity from a constructivist approach of international relations theory.
Keywords: cybersecurity, constructivism, cyber terrorism, cyberwarfare, ICT, cyber attacks, security policy

INTRODUCTION

Nowadays it's hard to imagine a world without Internet and computers. Our personal lives are dependent on these new technologies; our businesses and the global economy rely on ICT systems to carry out their communications and financial transactions. Both the private and the public domains are using global data networks to conduct businesses of hundreds of billions of dollars daily. By offering social services, education or critical health through ICT systems and networks, the public institutions are incredible dependant on these technologies to maintain their regular activities. And this dependency is likely to expand in the next period. The usage of new technologies is not offering us only benefits, they are also coming with a cost. As any device or technology, cyberspace has its vulnerabilities which can be quickly used by some individuals for personal,

economical, political and ideological gain (Cornish, Hughes and Livingstone, 2009).

The integrity of the cyberspace information is important not only to businesses or government, but also to regular citizens. Therefore, one of the main challenges of our times is defining a coherent cybersecurity policy which will prevent a possible complex large-scale cyber attack against our critical infrastructure and ICT. Even though cyber attacks do not have the dramatic image of an exploding bomb or a plane crashing into a building, they can seriously damage the government services, decrease people's trust in financial transactions, jeopardize business activity or break down the electronic communication system (Chertoff, 2008).

It is estimated that the number of devices connected to the Internet will rise to 15 billion by 2015. In this context, a safe and protected digital environment is a impetuous condition in order to acquire the benefits of the Internet. Thus, resolving the threats represented by vicious cyber actions is an important priority (Pawlak, 2013).

In this paper, I will try to present the current situation of cybersecurity and its cyber threats by offering to the reader a comprehensible understanding of the way through which ICT are influencing the security policy of governments, corporations or regular citizens. During this research, I want to find out if the concept of security in digital space can be explained by the constructivist approach of international relations theory. Thus, my research question is: **"Is cybersecurity the most important security issue of our century?"** and **"Does constructivism offers us a better understanding of the background, function and motives of cyber attacks?".**

The first part of the article will present the importance of ICT in our life and will develop the background of cybersecurity in correlation with the notion of cyber power. Moreover, the discussion will highlight the need for creating a coherent and practical cybersecurity which should be implemented in the national and international security legislation. The next part, describes the classification of cyber threats, with a special focus on hacktivism, cyber terrorism and cyberwarfare as the main important cyber crimes against the digital platforms of a state. The last part of the research tries to find a connection between the constructivist theory and cybersecurity and to offer to the readers a broad understanding of the subject. In addition, in this section I will try to explain why constructivism is the best approach when it comes to defining cybersecurity and cyber attacks.

FUNDAMENTS OF CYBERSECURITY

The 21st century will be defined by the implementation of cybersecurity in the national security agenda as a vital element in maintaining the status-quo of a state. If just a few years ago only the military had enough capabilities for causing large-scale demage, today anyone with adequete computer abilities can produce chaos and suffering within the major economies. As some experts evoke, the

world's arms race of this century will be about computer codes and not about fire arms (Al-Saud, 2012).

Up until 2007, cyber security was not a priority for national policy makers and thus many debates were more speculative than fact based. But in the last years, cybersecurity has become a strategic topic that started to acquire the attention of national policy makers, IT experts, diplomats, the intelligence community and military leaders in the pursuit of finding solutions to the threats that cyberspace has brought. Even though, it is not a new domain, it has increased incredibly and cyber acts have developed in sophistication and complexity. As Scott Borg affirmed, the digital environment has come to a phase were its defence demands the re-examination of every decision-making process, strategy, principle and manoeuvre (Borg, 2009).

Cybersecurity refers to the protection of systems, but also the protection of data from alteration, corruption or deletion. More than this, the data is also protected from unauthorized access and dissemination. As such, the ability of a system to perform as advertised is influenced by its safety, reliability and security (Computer Science and Telecommunications Board, National Research Council, 2002).

As a consequence of the increasing public attention to cyber threats, cybersecurity is the most important policy of the moment. From the cyber attacks on Estonia in 2007 to the industry-undermining super worm Stuxnet in 2010 and to the exposure of numerous cyberespionage cases by Snowden in 2013, it is clear that cyber perpetrators are becoming more sophisticated in their scams which are more recurring, more harmful and organized and more lethal in their attacks. Thus, counter measures to these cyber crimes had become top priority for many states around the globe, including the European Union member states (Dunn Cavelty, 2013).

Taking into consideration the current national legislation and policy framework in regard to cyber attacks, it is clear that due to the ever changing nature of cyber crimes an update of the national security policies is necessary. The major attacks from the past few years have demonstrated the possibility of undermining governments through attacks on the information infrastructure. President Barack Obama suggested that cyberthreats are "one of the most serious economic and national security challenges we face as a nation". Moreover, he argued that the economical prosperity of America during the 21st century is dependent on cybersecurity. Thus, the President called for an investigation of the federal government's role in protecting and securing the US information and communication grid (Brynko, 2013).

The Internet has brought to users tremendous benefits in communication, information, economic, political, social and cultural sectors but in the same time it can be a dangerous place where through the help of identity theft, viruses, malware, denial of service attacks, botnets or other cybercrimes hackers or cyber perpetrators (criminal, terrorist or extremist groups or even some states) can put in danger and threaten the security and citizens' trust in the Internet, thus, affecting the future of

it and its technologies. Except the case in which the states' private sector and international community will succeed to secure and limit the cyber criminal actions, there is a chance that the Internet and ICT will stop to grow and develop to their potential. So, sustaining the trust in cyberspace and online transactions and developing a safe online environment is impetuous for the proliferation and use of the Internet (Sund, 2007).

Keeping in mind the great interdependency and interconnectivity among sectors in cyberspace, it is difficult to decide which layer should be protected. Plus, as it is hard to distinguish which nodes and connection points need to be given a high priority, the tendency is to consider all of them critical infrastructure and fail to secure the most important layers existing in the digital space (Clemente, 2013).

The resilience of communication and electronic systems has become indispensable for all critical services in most countries. Telecommunications themselves are vital for the functionality of the present day society and with the rise of ICT, critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP) have become intertwined with cybersecurity and part of the international level politics (Sund, 2007).

CYBERPOWER

Since power is an important element in domestic or international affairs, it is important to see how cyberspace has affected this concept in correlation with national security. As Nye suggests, **cyberpower** is an ambiguous concept that has been described as an auxiliary tool to the existing hard and soft power categories (Nye, 2010). Or it represents the skills of using ITC and the Internet in order to gain political advantages, expecially by altering events in all other functional spaces and over all the remaining elements of power (Dunn Cavelty, 2013) .

Nowadays, citizens' lives are definitely changed by the rapid, easy and cheap communication networks which led to the change of general perception on power. The actors who control the information grid are the ones with an incredible power in cyberspace in our times. They can be IT companies which are altering the social norms for their self-interest or some totalitarian governments who control and censor the information available online for consolidating their power (Dunn Cavelty, 2013).

The importance of every single individual action was never this great as it is now in the digital environment. For example, in 2008, the U.S. millitary computers including those of the U.S. Central Command which were working on missions in Afghanistan and Iraq have been virused by a silent rogue program instaled from a flash drive by a foreign intelligence agent. The virus has been cyber spying on the American military computers and had transmited classified information to an unkown source. As the former Deputy Secretary of Defence, William Lynn sugested, it's the worst fear of a network administrator that some "rogue warriors" can affect America's global information grid, embezzle operation plans, weaken the intelligence information sources and hinder the weapons delivery process (Knowlton, 2010).

Thus, the classical perception of power and the ability to preserve and use that power in order to secure our environment has changed dramaticaly. Now, every actor who has the ability to use the computer in order to engage in cyber attacks, has automatily the power to affect the security of a state, institution or corporation and indirectly to influence the debate about the cybersecurity policy.

CYBER ATTACKS CLASSIFICATION

Many aspects of our modern life were changed in the last two decades by the Internet and ICT. According to the last Internet World Statistics, in 2012 there were almost 2. 5 billion users around the globe and this trend is increasing at a very fast speed (Internet World Stats, 2012).

The new technologies have spread the use of social networks (Facebook, Twitter, My Space etc.) which sustain the increased online risk. The posting of personal information on social networks represents a new kind of a security breach, as criminals can steal information through social engineering or spyware for financial crimes or identity thefts.

As software becomes more complex, there are more opportunities for attack. Thus, in the field of electronic businesses and government a reliable, secure network has become crucial and indispensable for the development of digital economy and performance of related ecosystems. Therefore, the users' trust in these technologies is tremendously important (Sund, 2007).

Cyber attacks vary from illegal low-level individual crime (hacking) to actions of non-state actors or groups (criminals and terrorists) to well organized attacks by state governments (Cornish, Hughes and Livingstone, 2009).

Because of various perspectives, the classification of cyber incidents is challenging and dependent on the involved actors' beliefs. Hence, Major Adkins considers that cybersecurity includes cybercrime, cyber espionage, hacktivism, cyberwarfare and cyber terrorism. According cu Veerasamy and Taute, there are: cybercrime, cyber terror and information warfare. In addition, as one report from 2009 of CRN[1] suggests, the actors engaged in cyber attacks are "terrorist organizations, organized criminal and state-sponsored actors", "established capable states" and "online criminals" (Tikk, 2011).

Plus, some authors consider that the most common cybersecurity threats are represented by:

- Online identity theft
- Industrial cyber espionage
- Critical infrastructure protection
- Botnets[2]

[1] Crisis and Risk Network (CRN) is part of the Center for Security Studies (CSS), ETH Zürich.

[2] Botnets, as defined by Moore, are *"a network of thousands or even millions of computers under the control of an attacker that is used to carry out a wide range of services. The services include sending spam, committing online-advertising fraud, launching denial-of-service attacks, hosting phishing attacks and anonymizing attack traffic".* (Moore, 2010)

In the opinion of Dr. Lachow, there are different ways through which hacktivism, cybercrime, cyber terror, state-level info war, cracking and cyber espionage have buit their motivation, methods and targes (Tikk, 2011).

Through **hacktivism,** we understand the merging of activism with hacking which is displayed by the disfigurement of websites with political and social messages or denial-of-service (DoS) attacks that interrupt access to the targeted websites. According to Denning, the nationalistic and patriotic hacking doesn't enter in the same category as hacktivism because it represents the acts of the individuals (citizens, expatriates) engaged in online actions in order to defend the motherland. These attacks are primarily addressed against e-mail accounts and websites of those states which have threatened or harmed their country of origin (Tikk, 2011).

	Motivation	Target	Method
Cyber Terror	Political change	Innocent victims	Computer-based violence or destruction
Hacktivism	Political change	Decision-makers	Attack
Cracking	Ego, personal enmity	Individual, companies, governments	Attack, exploit (sometimes overt)
Cyber Crime	Economic gain	Individual, companies	Fraud, ID theft, blackmail, attack, exploit
Cyber Espionage	Economic gain	Individual, companies, governments	Attack, exploit (rarely overt)
State-Level Info War	Political or military gain	Infrastructure, military assets	Attack, exploit, physical attack

Figure 1: Lachow's Chart. Availabe at (Tikk, 2011, 58)

Cyber attacks by hackers are increasingly growing more sophisticated, keeping the pace with anti-viruses and other security measures and have been customized for specific targets. At a personal level, hackers are less motivated by fame but by money or revenge. VeriSign Intelligence has estimated that in 2007 the main threat to networks has been espionage (VeriSign, 2007).

Due to the anonymous and confidential character of the Internet, it is very attractive to illegal and criminal organizations also. Plus, as these organizations become more complex and opaque, their identification and tracking is significantly more difficult. The structures of these types of organizations are believed to be

"*networks within networks, connections within connections and links between individuals that cross local, national and international boundaries*" (Cornish, Hughes and Livingstone, 2009).

There are states and criminal groups who have the technical capabilities to target private and governmental information networks with the purpose of stealing commercial or security secrets and acquiring competitive leverage in those sectors. According to the US intelligence experts, Russia and China are among those nations who have these capabilities.

The first massive cyber attack against a country is considered to be the attack on Estonia's governmental ICT infrastructure, banking system and Internet providers in 2007. This episode had erupted as a consequence of a dispute between the Estonians and Russian minority over a Russian war memorial in Estonia. It is not clear if it was a spontaneous attack from the Russian computer users or an action planed by the Russian authorities. But the message of this event is clear, even the biggest companies or national departments cannot escape from being targeted by Distributed Denial of Service (DDOS) attacks or **"clickskrieg**" as they are also called (Cornish, Hughes and Livingstone, 2009). This was the trigger that has contributed to NATO's decision of building a Cooperative Cyber Defence Centre of Excellence in Estonia.

CYBERSECURITY LEGISLATION

Every day, almost 144 000 malicious files are detected; this sums more than 4.3 million files every month. Therefore, the fight against illicit cyberthreats should be constant and ongoing alike the constant war on crime (Chirantan and Sprague, 2012). Cybercrime has grown in the last years also due to our addiction to purchase new devices whose mobile technology or cloud computing services have a relatively poor security (Chirantan and Sprague, 2012).

As Patrick Lincoln, director of the computer science laboratory at SRI International said, the bad guys are improving more quickly than the good guys. If we take the case of the United States, the illicit economic cyber activities cause a loss of $100 billion to the economy every year (Baker, 2009).

Attempt to regulate the cyber crimes at international level led to the lauch of Council of Europe Convension of Cybercrime in 2001 (also known as Budapest Convension on Cybercrime). This represents the first international treaty which by harmonizing national laws tries to aim computer crime and Internet crimes (Weber and Heinrich, 2012). But as some authors suggest, this treaty prezents a lot of flaws because:

Being based on criminal cyber-conducts in the late 1990s the Convention on Cybercrime does not cover new methods of conduct in cyberspace with criminal intent, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of the Internet, and massive and coordinated cyber-attacks against information infrastructures. In addition, the terminology included in the Convention turns out to be a 1990s terminology which is not necessarily suitable

for the second decade of the 21st century. Hence, with regard to the use of anonymizing services on the Internet the Convention on Cybercrime contains no specific regulations; the Convention ''solely'' introduces a regulatory framework for its Member Countries to handle criminal actions related to the World Wide Web. (Weber and Heinrich, 2012, 56)

The increasing dominance of new technologies in communications had given rise to two different perspectives about the future of the Internet. On one side, there are the liberal democratic states (US, EU) which promote a multi-stakeholders approach in which governments should cooperate with civil society, private sector and technical experts to render the fondation of Internet governance. On the other hand, there are the "cyber-sovereignity" group of states (Russia, China) which wish to control and limit the Internet (Pawlak, 2013).

The International Telecommunication Unit (ITU) have started organizing World Summits on the Information Society under the patronage of the United Nations. Both World Summits on the Informational Society held in Geneva and Tunis have emphasized the importance of security in constructing a secure global information society. Thus, the ITU together with actors from governments, civil society, private sectors and international organizations have founded the Global Cybersecurity Agenda (GCA) on the 17th of May 2007 trying to stimulate cooperation between all relevant actors involved in this subject. In order to accomplish its purpose, the international law should start including serious cyber crimes, despite the fact that they are indictable under the national law (Weber and Heinrich, 2012).

The effects and impact of cyber attacks can be seen also through the measures adopted by both states and international organizations: NATO's Cyber Defence Policy and Strategy (2008), EU's Communication on Critical Information Infrastructure Protection and proposed Directive on Attacks against Information Systems. Also this subject has reopened discussions at the level of the UN regarding information security and data protection (Tikk, 2011).

CYBERTERRORISM

It is important to highlight that cyber threats are affecting the state, public areas, the private domain and individuals in the same manner and with the same intensity. As an evidence of the globalised society, not only the businesses and nations are using the new technologies in their everyday activities but also the illegal sector has moved online. In present, terrorist groups like Al Qaeda, Hamas or Hezbollah have started using ICT in their work. Moreover, cyberspace criminality is growing and has become more complex and elaborated in targeting and conducting extensive illegal cyber services which are available to the highest bidder (Chertoff, 2008). Because the online environment is an anarchic or ungoverned space, the extremists are profiting from its characteristics as any other citizens, for communication, information and sharing usage.

Cyberterrorism is terrorism in cyberspace. As such, it includes attacks and threats to the communication infrastructure and the data from within, executed with the aim of applying fear and intimidation in the support of a socio political agenda. Therefore, to be qualified as an act of cyberterrorism, an attack should cause significant damage, injuries or deaths, financial and economic loss (Weimann, 2004). As Talihärm points out, cyberterrorism was a notion so badly understood that there were many voices that doubted it was even a threat (Talihärm, 2010).

Cyberspace is now perceived as the "most important meeting place for jihadis all over the world to communicate, discuss and share their views" (Cornish, Hughes and Livingstone, 2009). Moreover, the extremist websites are expanding quickly, with a birth of thousand of websites per day. The cyberspace offers them the setting for cheap, rapid, clear, coded and stenographic communication. Through the usage of websites, blogs, forums, social media channels, the Internet is allowing them to spread and debate ideas, various techniques and to do virtual trainings. In this way, the Internet is a good channel for the creation and dispersion of propaganda. Besides this, all the messages posted online can sum up all the political, religious and ideological ideas that form a virtual library of propaganda communications (Cornish, Hughes and Livingstone, 2009). Cyberspace has also became a space for instruction and teaching where these extremist groups are taking their "virtual training camps".

CYBERWARFARE

Information and communication technologies have also influenced warfare by giving rise to a new field of warfare: cyberwarfare. In the post Cold-War period, war is fought in different types of battlefield because of the influence of the non-state actors which have moved some of their actions in cyberspace. With the help of the global media, these actors have also started a war of perceptions, information and electronic deception. The former battlefield was changed for a "battlespace" which includes alongside the three dimensions of land-sea-air power plus the use of space satellites, a non-dimension area, represented by cyberspace and communications wavebands (Baylis, Smith and Owens, 2011).

As states become more dependent on complex information-gathering and weapon-targeting technologies and command systems, they become vulnerable to cyber warfare. Cyber space is "the total interconnectedness of human beings through computers and telecommunications". Cyber warfare therefore relates to a state's ability to attack another state's computer and information network in cyberspace and to protect its own capabilities from attacks by adversaries. This is critical in contemporary high-technology warfare, where the USA, for example seeks to dominate the information domain so totally in wartime that it can conduct its military operations without effective opposition. Such attacks can be limited to purely military targets or can be directed against the adversary's economic and political system more generally. A large number of states such as India and Cuba are believed to be developing cyber warfare capabilities and several, including the

USA, Russia, China, and the UK, have incorporated cyber warfare into their military doctrines. (Baylis, Smith and Owens, 2011, 217)

It is considered that cyberwarfare is the most significant security threat of cyberspace. In this regard, ICT can be used for targeting the state's institutions, financial nodes, energy sector and transport infrastructure or to create mass confusion or panic. It is important to highlight that not all cyberwarfare attacks are intended as acts of war. We have to distinguish between warfare and non-warfare in cyberspace. To do so, it's vital to take into consideration the gravity of the attack, its warlike properties and the actor involved. Even though some threats of terrorists groups, spies and organized crimes can be destructive, not all of them are designed as cyber warfare actions (Cornish, Livingstone and Clemente, 2010).

Cyber war can represent a conflict between nations but also non-state actors can get engaged in different ways. In this type of conflict the oponents can be military, industrial or civilian. The most esential characteristics of cyber warfare are (Cornish, Livingstone and Clemente, On Cyber Warfare, 2010):

- It offers excessive power to small and irrelevant actors that in other circumstances would not matter;
- It facilitates actors to carry on their strategic and political agenda without engaging in an armed conflict;
- In the online environment the borders are blurred among the physical and virtual and between the military and civilian space. Power, here, can be employed by nations, non-state actors or by proxy.
- Perpetrators can work anonymously and unpunished for some time by using false IP addresses, aliases or foreign services.
- The warlike actions in cyberspace have more chances to appear in correlation with other types of conflict. However, its means and particularities are distinctive from traditional warfare actions.
- Cyberspace is perceived as the "fifth battlespace" besides land, air, sea and space.

The terrain for cyberwarfare (cyberspace writ large) is in a continuing process of alteration and growing. As cyber attacks rarely are caught, the offensive position instead of a static defensive one is the most recommendable for protection.

The 2008 Georgia-Russia conflict was the first military action which had a cyber element. Simultaneously with the Russian military attack on Georgia, there have been launched cyber attacks which have blocked the Georgian governmental websites and had reduced the access to public communications and services (Chertoff, 2008). It was described as "the coming of age of a new dimension of warfare" Even though the DDOS attacks on Georgia had not long-term cyber damages, it is clear that this kind of coordinated attacks on the Internet have a lot of potential for causing mass confusion and fear (Cornish, Hughes and Livingstone, 2009).

CYBERSECURITY FROM A CONSTRUCTIVIST POINT OF VIEW

Constructivism is an international relations theory which has proposed the rethinking of the international relations as a particular species of human relations. The premise of this approach is considering that the processes of identities and interests formation happen in the same time with the process of interaction. The constructivist authors start with understanding the individual and social relations and after will extend their focus upon the institutional and international levels (Mişcoiu, 2007).

We are approaching a new security paradigm because of the numerous consequences which led to various changes in the logic and nature of current security practices. Until now, the national security was acknowledged as the government's incumbency and was dependent on foreign policies, the intelligence community and military capabilities. Nevertheless, today the critical infrastructure is conceived as a shared responsibility where the government itself cannot offer the necessary security (Eriksson and Giacomello, 2004). Thus, sustaining the engagement of private, local or individual actors in the networks security has the same importance as the national or international attempts in protecting the digital environment.

As such, we have a new framework were security is a speech act. The theory of securization was developed by the Copenhagen school. This is resumed as:

A securizing actor by stating that a particular referent object is threatened in its existence claims a right to extraordinary measures to ensure the referent objects survival. The issue is then moved out of the sphere of normal politics into the realm of emergency politics, where it can be dealt with swiftly and without normal (demographic) rules and regulations of policy making. For the content of security this means that it has no longer any given meaning but that it can be anything a securitizing actor says it is. Security – understood in this way- is a social construction, with the meaning of security dependent on what is done with it. (Baylis, Smith and Owens, 2011, 240)

During this chapter, I will combine the constructivist notions with examples from digital world in order to discover an answer to my research question.

I will start by saying that the actors' actions and reactions are influenced by their perception of the environment, including the technological space and the outcomes of it. The threats are social constructs because the concept of social threat didn't exist before the process of interaction. In addition, the identities are the ones which form collective understandings starting from a particular case and developing it through socialization (Wendt, 1999). As an example, the current decisions regarding cybersecurity and attacks are created upon assumptions and scenarios since we don't have a precedent of a destructive cyber attack. Because different stakeholders are engaged in this process, from the ICT industry to various

state agencies, along with their views, perceptions and interests, there is a certainty that every one of them is trying to impose their ideas regarding the way of constructing the future type of cyberspace. Therefore, the national security concept is based, nowadays, more than ever upon perceptions regarding the real threats and imagined ones (Eriksson and Giacomello, 2004).

Accordingly, we take into consideration that an institution is a stable set of norms and structures of interests and identities. Plus, it is a cognitive entity which takes shape only through actors' ideas of how to interpret the world. And these institutions have impact only through actors' socialization process and through participation at the collective knowledge (Wendt, 1999). We can state that cybersecurity is definitely an institution under formation where the actors have to collaborate in order to establish a new set of norms and international legislation that will help the international community to protect itself from cyber perpetrators and to find ways of punishing them.

Cybersecurity threats have changed the social structures of security and conflicts, their norms and participation rules. In cyberspace, the social structure of violence is blurred and the line between civilians and combatants are unclear. Hence, an interpretation of the current cybersecurity policy and its threats from a constructivist point of view can be an interesting experiment which will help us to better understand the events and actions from cyberspace.

Some motives of the actions of cyberspace perpetrators can be explained by the willingness of that actor to dominate, gain a strategic or political advantage or to substantially harm a state or population in pursuing financial benefits or self-interest (Cornish, Livingstone and Clemente, 2010). The online environment is the most appealing space for following cultural, ideological, religious, economic, social and political agendas. It is interesting to highlight that extremist or terrorist websites do not present any information regarding violent actions, suggesting that appealing to violence is the last resort. Instead, they describe themselves as persecuted, that their followers were murdered and their leaders have been victims of assassinations. This type of approach is given by the terrorists and extremists groups in order to sensitize the audience and to lead them to the idea that they are weak, outsiders and misjudged (Bogdanoski and Petreski, 2013).

Symbolic politics are present on the internet also. For example, defacing websites is symbolically similar to flag burning as it denigrates and destroys national symbols and pride, with more damage to the image and confidence than to the financial side of the victim. Such actions affect the trust, appreciation and strength of the users in their networks but also give birth to the need of revenge. In addition, if we keep in mind the constructivist notion of "looking-glass self" (which suggest that one actor's actions reflects other actor's reaction), in this way, we can understand why many American hackers respond with the same actions if Chinese hackers attack the U.S. governmental websites and why these acts are perceived as an affront and outrage to their national pride (Eriksson and Giacomello, 2004).

Compared to air, sea, land and space, the cyber environment is exclusively human-made and determined by political and economic pressures. It is vital to highlight that any serious security exposure can be a result of fallible technical or human connections in the whole system. Moreover, due to the fact that security contains substantial administrative, procedural, physical grid and personnel components, it represents partial a technical issue (Computer Science and Telecommunications Board, National Research Council, 2002). The digital space is not just a single network; it is formed by numerous networks each with its particular characteristics and norms controlled directly or indirectly by different nations (Dunn Cavelty, 2013). Individual and organizational users are expecting from their computer:

- confidentiality (in terms of controlling who can read the information),
- integrity (the assurance that changeable character of information and programs is safe and authorized)
- availability (the assurance that the authorized users have permanent access to the information systems and programs).

These three features best describes what regular user needs regarding their information security and trust in networks (Computer Science and Telecommunications Board, National Research Council, 2002).

The ontological security refers to some ethical, moral and identity values which contribute to the formation of a national cohesion in a community (Wendt, 1999). The self's security is the core of ontological security and every individual needs a stable image about itself in order to be able to act and interact. If this image around which he had constructed his entire perception of his identity is removed, it will make him unable to take any decisions, feel anxious about his environment and live always in uncertainty (Mitzen, 2006). Cyber terrorism exploits two great fears of our society: the fear of random and fierce victimization and the fear of computer technology, both which are different sides of the fear of the unknown. Fear of terrorism derives from its random, unmanageable and inexplicable nature, while computer technology is feared because of its complex nature and perceived threat to human jobs. Hence computers have taken the human's place in certain activities, there is the threat that technology can be "out of control" and this perception is fed by the growth of ICT in entanglement and connections (Eriksson and Giacomello, 2004).

One of the effects of digital warfare is the distancing from the cruel realities of war. Through the "digital glass" war is seen more like a computer game, a simulation, thus reality and imagination are more and more overlapped. In these conditions, the perceptions on running a war are altered by the digital space. The similarities between digital war and computer games are tremendous thus making it hard to differentiate between a real attack and a game since the perceptions and the actions are almost the same (Eriksson and Giacomello, 2004). As such, it is not surprisingly that the military is more interested in the videogame and film industries.

Information warfare can be perceived as "identity warfare" where the domestic-international divide is challenged, the boarders are blurred and the identity of the nation-state is contested but there is also the possibility that nations will adapt and not crash under the new identity paradigm formed by cyberspace and its tendency to blur lines and boarders (Eriksson and Giacomello, 2004).

In cyberspace, there are different terms and rhetoric that are constantly used. As such from the constructivist point a view, the use of terms such as "bugs", "viruses", "worms", "firewalls" makes the cyberspace more comprehensible and familiar. Also the use of strong symbolism such as an information "warfare", and "electronic Pearl Harbor" illustrates the perceived impact of digital actions - comparable with the one from conventional conflicts.

In any structure made from ideas, there will be some ideas which will be shared and other not. The shared ones, especially about the Self and Other, are forming the political culture of an international system. The political culture is one of the most important concepts which help us to better understand the mechanism of the international society. Wendt identifies three different periods of political cultures of anarchy: the Hobbesian culture, the Lockean culture and the Kantian culture. From these three, the last one is the one who is actively promoting collaboration in the international system. Here the security of one member is considered as the security of all its members. The individual or national interest is viewed as the interest of all stakeholders, thus cooperation and partnership is possible (Wendt, 1999).In order to create a credible and trusting network system, there should be more than one line of defence, a series of intersected defences containing public and private norms, national and international policies and bilateral and multilateral cooperation arrangements. Only in this situation, the users will have the comfort of a backup in case of breaches. When developing cyber defences, the issues are addressed from several points of view: technical, economical and legislative and also from the national security point of view, depending on the actors' role, influence and interest (Sund, 2007).

To reduce the possibility of cyber threats, the government should cooperate with the private sector and also adopt and implement a clear and flexible cybersecurity policy in all its domains. Moreover, it should work on increasing the monitoring capacities and intergovernmental agencies collaboration. As for the civilian networks, they should have the necessary levels of security to be able to enter on the Internet because every weak link can expose the entire system (Chertoff, 2008).

It is important to notice that the Internet and the social and commercial online activities will deepen and grow if only users will trust the networks not to lose their personal information and identity when they are entering cyberspace. For building this user confidence in ICT, we'll need multiple partnerships between the public and private sectors, businesses, holders and operators of cyber infrastructure and individuals (Chertoff, 2008).

CONCLUSION

At global level, in 2012, there were approximately 30 million cameras installed in places ranging from ATMs, shopping malls to parking lots which have captured 250 billion hours of unprocessed footage (Lee, 2013). As Bruce Schneier has logically afirmed, the year 2013 represents a turning point in the threat perception when problems like state's cyber-exploitation have started to take the floor of the current debates about cyberspace and cybersecurity (Schneier, 2013).

The current debate is fought around the idea that too much information is displayed in the digital space and this fact raises many security questions. For example, according to the FBI, the group who tried to detonate a car bomb in Times Square on the 1st of May 2010 was aided in their reconnaissance activities by public web cameras. As a consequence, Google Maps has blurred and digitally modified its satellite pictures of some important landmarks such as the White House, NATO air force hubs etc. (Lee, 2013).

Technological advances play a major role in the changing of humanity by defining its history, institutions and human actions. Also, there have been other information and communication revolutions with clear impact over human affairs, such as the way in which communications are shaped by the use of new digital devices.

This paper started with the aim of demostrating the urgent need to include cybersecurity in the national and international legislation and to find ways through which the networks should be protected against cyber attacks. Moreover, the discussion brings in the readers attention the danger of the Internet and its usage in hurting others, stealing information, causing panic and fear through simple actions such as blocking the online public services and governmental websites.

If national security policy was based upon military capabilities, intelligence gathering and foreign affairs, in our days, it has to include the fact that the information and communication grid has to be protected against cyber perpetrators.

At the begining of this research, I have stated the desire to find some answers to the questions: "*Is cybersecurity the most important security issue of our century?"* and "*Does constructivism offers us a better understanding of the background, function and motives of cyber attacks?".* Throughout this paper, I have presented the cybersecurity concept along with its features, importance, threats and effects on everyday life from a perspective focused on the state. Thus, I have explained the main cyber security dangers to a state, such as cyber terrorism and cyberwarfare and gave examples of these kinds of attacks. I do consider that cybersecurity is the most important security issue of our century because it doesn't only affect the ICT networks but also it hurts economies, military capabilities and intertwines in governmental actions and reactions. Regarding the second question, the use of constructivism in defining cybersecurity and explaining its elements facilitates a greater understanding of this matter. This perspective offers us more explanations regarding the security of digital space, the impact of ICT on national security and the interpretation of cyber threats than any other theory of

international relations because it focuses on ideas, perceptions and structures as flexible social constructs which are in an ever changing situation.

BIBLIOGRAPHY

1. AL-SAUD, Naef Bin Ahmed, *A Saudi Outlook for Cybersecurity Strategies Extrapolated from*, in *Joint Force Quarterly*, No. 64, 2012.
2. BAKER, David, *President Obama's Chilling Cybersecurity Challenge*, January 6, 2009. http://www.astd.org/Publications/Magazines/The-Public-Manager/Archives/2009/01/President-Obamas-Chilling-Cybersecurity-Challenge (accessed March 10, 2014).
3. BAYLIS, John; Steve SMITH, Patricia OWENS (eds.), *The Globalization of World Politics, An introduction to international relations*, 5th Edition, Oxford University Press, New York, 2011.
4. BOGDANOKSKI, Mitko, Drage PETRESKI, *Cyber terrorism– global security threat*, in *Contemporary Macedonian Defence - International Scientific Defence, Security and Peace Journal*, Vol. 13, No. 24, July 2013.
5. BORG, Scott, *The Cyber-Defense Revolution – A Synthesis*, in *NATO Cooperative Cyber Defence Centre of Excellence*, 2009. http://www.ccdcoe.org/cyberwarfare/images/234.pdf (accessed March 11, 2014).
6. BRYNKO, Barbara, *Cybersecurity: You've Been Hacked*, in *Information Today*, June 2013. http://www.infotoday.com/IT/jun13/index.shtml (accessed March 7, 2014).
7. CHERTOFF, Michael, *The cybersecurity challenge*, in *Regulation and Governance*, No. 2, 2008, pp. 480-484.
8. CHIRANTAN, Desai, Steven SPRAGUE, *Are we winning the cybersecurity war*, in *NetworkWorld*, February 13, 2012. http://www.networkworld.com/community/node/79628 (accessed March 15, 2014).
9. CLEMENTE, Dave, *Cyber Security and Global Interdependence:What Is Critical?*, Chatham House, London, 2013.
10. Computer Science and Telecommunications Board, National Research Council, *Cybersecurity Today and Tomorrow*, National Academy Press, Washington, D.C., 2002.
11. CORNISH, Paul; David LIVINGSTONE and Dave CLEMENTE, *On Cyber Warfare*, Chatham House, London, 2010.
12. CORNISH, Paul; Rex HUGHES and David LIVINGSTONE, *Cyberspace and the National Security of the United Kingdom, Threats and Responses*, Chatham House, London, 2009.
13. DUNN CAVELTY, Myriam, *A resilient Europe for an open, safe and secure cyberspace*, Stockholm: The Swedish Institute of International Affairs, 2013.
14. ERIKSSON, Johan and Giampiero GIACOMELLO, International *Relations Theory and Security in the Digital Age*, in *International Studies Association Convention*, Montreal, 2004.

15. Internet World Stats, *Internet Usage Statistics*, June 30, 2012. http://www.internetworldstats.com/stats.htm (accessed March 2, 2014).
16. KNOWLTON, Brian, *Military Computer Attack Confirmed*, in *The New York Times*, August 25, 2010. http://www.nytimes.com/2010/08/26/technology/26cyber.html?_r=0 (accessed March 17, 2015).
17. LEE, Newton, *Counterterrorism and Cybersecurity, Total Information Awareness*, Springer, New York, 2013.
18. MIȘCOIU, Sergiu, *Câteva răspunsuri la întrebarea 'De ce a avut succes socio-constructivismul ca teorie a relaţiilor internaţionale?*, in *Direcţii principale în studiul relaţiilor internaţionale*, by Ruxandra IVAN, Institutul European, Iași, 2007.
19. MITZEN, Jennifer, *Anchoring Europe's civilizing identity: abits, capabilities and ontological security*, in *Journal of European Public Policy*, Vol. 13, No. 2, 2006.
20. MOORE, Tyler, *The economics of cybersecurity: Principles and policy options*, in *International Journal of Critical Infrastructure Protection*, No. 3, 2010.
21. NYE, Joseph, *Cyber Power*, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (accessed March 20, 2013).
22. PAWLAK, Patryk, *Cyber world: site under construction*, Brussels : European Union Institute for Security Studies, 2013.
23. ROBERTS, Nancy; Richard HARKNETT and James STEVERteve, *The New Policy World of Cybersecurity*, in *Public Administration Review*, May 2011.
24. SCHNEIER, Bruce, *The Battle for Power on the Internet*, October 24, 2013. http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/ (accessed March 11, 2014).
25. SUND, Christine, *Towards an international road-map for cybersecurity*, in *Online Information Review* , Vol. 31, No. 5, 2007.
26. TALIHÄRM, Anna-Maria, *Cyberterrorism: in Theory or in Practice?*, in *Defence Against Terrorism Review* (Center of Excellence-Defence Against Terrorism), Vol. 3, No. 2, 2010.
27. TIKK, Eneken, Comprehensive legal approach to cyber security, Tartu: Tartu University Press, 2011.
28. VeriSign, *A Holistic Approach to Security Intelligence*, August 21, 2007. http://www.verisign.com/static/037640.pdf (accessed March 2, 2014).
29. WEBER, Rolf H. and Ulrike I. HEINRICH, *Anonymization*, Springer, London, 2012.
30. WEIMANN, Gabriel, *Cyberterrorism.How real is the threat?*, United States Institute of Peace, Washington, 2004.
31. WENDT, Alexander, *Social Theory of International Politics*, Cambridge University Press, Cambridge, 1999.