THE CYBER THREAT AND THE PROBLEM OF INFORMATION SECURITY

A critical analysis of the concepts of cyber-power and cyber-space

Sebastian SÂRBU*, PhD

Abstract: *In this paper we approached from a researcher's angle and analyzed the concepts of cyber-space, cyber-power from the security school perspective, from that of the international organizations, and from the civil society point of view. Therefore we referred to the documents and the international initiatives concerning the security of data transfer in the context of the current threats against cybernetic security on the one hand, and its interpretation as a threat to the values, rights and democratic freedoms of the civil society, on the other. The risk society is defined both through the grid of political sociology, of the Copenhagen school, as a key element of reference in this case, as well as through the necessity to build a safe cyber space, here being scrutinized in a value-based antithesis between terror and democracy / freedom of speech. Data security and control and also the internet-based data transfer are approached in this article from the angle of the European documents, but also from the perspective of the civil society, emphasising the regulatory efforts made by authorities and the civil campaigns. In turn, cybernetic attacks are studied from the angle of the NATO strategic concept and also from the perspective to be found in the UN and EU documents. As for the cyber-power concept, this finds its „implementation" inside the sphere of the geopolitical world, being quite relevant in the security vulnerabilities of the software constructs, of the international and local networks. Also, cyber power is associated with cyber-espionage, cyber-war, cyber-criminality and cyber-space.*

Key words: *cyber-war, cyber-terrorism, cyber-space, cyber power, cyber-criminality, cyber-weapon, cyber-espionage, cyber-war, the Copenhagen school, risk society, data safety, data transfer, information control, critical infrastructures ACTA.*

* Researcher, member of the Interdisciplinary Research Group of the Romanian Academy, vice-president of the National Security Academy for Defense Planning, Special Advisor Helsinki Think Tank, member of the Romanian Society of European Law.

In NATO's Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon, 2010, we find the following text at the 12th paragraph („The Security Environment" chapter):

„Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks."

In fact, the increasing number of attacks is the result of the growing number of software being used, as well as of Internet users, and not an endemic fact or one linked to an increase of cyberspace aggressiveness. The vulnerabilities of a single application can be exploited by using the same tactics on a wide range of similar implementations. What is most striking is rather the poor quality of applications, as well as implementation flaws, the absence of legal framework for consumer protection, software being the only (legal) merchandise not being subject to quality regulations. Standards of quality in the software industry are a subjective unit generally measuring extended functions and post-sales assistance services.

Costs are growing as the number of users utilizing the same vulnerable (and possibly badly implemented) application increases.

In another recent NATO document mentions are made about difficulties generated by lack of consensus regarding the definitions of terms associated with the threats and consequences of certain actions in cyberspace. Similar difficulties can be observed in defining terrorism, although a UN resolution is trying to solve the problem. Nonetheless, interpretations are rather subjective and vary from one country to another.

For example, the USA, openly fighting against terrorism in multiple war theatres, after more than 11 years, were unsuccessful in properly operationalizing the terrorism-linked definitions in cases such as: the legal status of people captured in its operations; a legal formal framework concerning their treatment during detention; or their legal status once they are set free. Conceptual definitions are susceptible to transformation with time, on relatively short intervals, and may be partially replaced by other

conceptualizations, varying by region. It is important to mention this precedent for it establishes without doubt that the absence of international consensus does not lead to an absence in a strategy's operativeness, at least not unilaterally.

Cyber-war, cyber-terrorism, cyber-espionage, and cyber-crime refer to the same set of events, the differences being rather syntactic. Despite laws against cyber crimes, the problem of cyber-aggression entered largely under military scope. Although legal definitions are generous enough to cover all these events (unauthorized access or preventing authorized access to data or information systems is a crime), instituting a new conceptual background (via these „cyber" derivatives) renders military action to substitute civil legislation.

In the same NATO study, certain questions are posed:

- when is a cyber attack an act of war and when is it a crime?
- when is unauthorized access to computer systems a cyber attack?
- what are cyber weapons?
- how does the victim of the attack identify the aggressor and what degree of confidence is necessary for positive identification?

In the document, cyberspace is defined as the national environment where digital information is stored or transmitted via information systems and networks. A first objection to this definition relates to the national character of information. Since information systems (or networks) make no distinction between information and execution codes, their interpretation is linked only to the subject, a certain set of instructions being considered both data and information carriers. How can certain data carry (symbols of) nationality? The only possible valid response is linked to the physical environment it passes through: if it is located on a certain territory then the data is considered to belong to that territory. The speed at which data travels, as well as other characteristics of data transportation, give it a time-frame of a few milliseconds. Another problem is linked to the source: if the source is a „foreign" code (generated by an information system in a pre-programmed fashion), does the data keep its territoriality/nationality?

In a Ph.D. thesis (this time from Romania) centered on the problem of cyber terrorism, the author tries to systematize the terms used:

„The concept of 'cyber-terrorism' refers to utilizing tactics and techniques of information warfare by terrorist organizations, thus affecting

cyberspace. The cyber terrorist operates exclusively in the virtual space and does not physically destroy the infrastructure rendering possible the existence of virtual space. While information terrorists aim for an impact on the actions of 'real' people in the 'real' world, they operate inside the virtual world of cyberspace in order to manipulate these actors."

As we can easily see, the three sentences contradict and exclude each other: warfare tactics and techniques are (by admitting their nature) attributes of the military (calling it 'information' warfare is even more ambiguous, and we will not discuss this aspect), not of terrorists; the phrase „affecting cyberspace" is contradicted by the following sentence („does not physically destroy [...] virtual space"), the impact being on the „real" world, as if cyberspace were fictitious.

In the Lipman Report, published in the latest edition of „Foreign Affairs" (November 2010), the definition of cyber terrorism is closer to that of the „classical" one but just as ambiguous: cyber terrorism includes „the fear of terrorist violence". The tautological aspect of the phrase („fear of terrorist violence") should not prevent us from identifying a reality: technology is not violent, nor information infrastructure or systems (despite the appearances). If we were to accept this definition for IEDs (improvised explosive devices), then mobile phones would also be terrorist, and the possible term of „tele-terrorism" would challenge even more the intelligence of the readers.

The context of international initiatives for cyber security

In the USA, the initiative to secure cyber space became the responsibility of a four-star army general, Keith Alexander, in the newly-formed USCYBERCOM. When instated he expressed his vision: „the only way to counter the threats of online crime and espionage is via a proactive attitude". Immediately afterwards, he brought into discussion the Chinese threat to electricity networks (generally and particularly) in the United States – a threat cited (including in the press), with very few exceptions, in all discourse referring to cyberspace and cyber security (Wikipedia, 2011).

USCYBERCOM has competences in the sector of military communications, but according to its statute, intervention in civil communication networks may be operated when solicited by the President. It is extremely difficult to operate with sectorial notions in the field of

Internet communication, given the exhaustive nature of the concept (the Internet represents all the public communication networks using TCP/IP protocol), and thus a sector is impossible to identify, since it belongs to the whole (Internet) by the very nature of its (technical) behavior.

NATO has included in its security strategy, alongside the (increasing) necessity of collaboration with Russia, a defense component against cyber warfare, without omitting, when announcing its policies and objectives, an offensive component.

The NCIRC (Computer Incident Response Capability), created in 2002, deals with security incidents and disseminates information about incidents. The structure is a part of NATO Communications and Information Services Agency.

The CCDCOE (Cooperative Cyber Defence Center of Excellence), created in 2003 and accredited as a NATO center of excellence, performs training in cyber warfare techniques.

The CDMA (Cyber Defence Management Authority) coordinated cyber defense in the Alliance.

ENISA, a recently founded EU agency, offers counseling on cyberspace security problems, by (as described) reaching an effective, high level of network security in the Union.

Romania also included in its Strategy for National Security, in the chapter „Main risks and threats to Romania", cyber terrorism and/or virtual environment propaganda, listed before the threat of weapons of mass destruction, ballistic development programs, etc. Romania has (surprisingly) a recent history filled with cyber security problems (Cyber Bucharest). During the NATO summit in Bucharest, in 2008, the President presented during a „private" meeting a series of documents regarding future NATO strategy for cyberspace security. While there is lack of public knowledge on the nature of these documents, a part of the subject is presented as having being in connection with the events in Estonia, in 2007.

In NATO terms, the purpose of a cyber attack is represented by two distinct (and somewhat contradictory) objectives:

- copying, then deleting data without affecting the system or data (passive attack - AP);

- affecting cyberspace by corrupting or modifying data, affecting the functioning of systems or communication networks, or preventing usage of systems or networks (active attack, destructive in character - AC).

Both definitions are included in the texts of information crime legislation (except for contradictory matters).

USDOD's definitions for the two categories in NATO terms are: computer network exploitation (CNE); and computer network attack (CNA).

AP and CNE, and AC and CNA, respectively, are equivalent. The AP/CNE class includes cyber crime, cyber espionage (if government actors are involved), and cyber terrorism (if the agent is an individual or terrorist group).

The objections to these definitions are primarily linked to their legal aspect. Neither governments, nor individuals or groups can refuse to abide by current legislation. No matter the nuances of the definitions emphasizing the agent (individual, group, state) or the action it provokes (cyber terrorism, cyber espionage, etc.), laws are applicable in a nondiscretionary fashion under the auspices of constitutionality. Another objection refers to the purpose of the action (copying, deleting, or blocking access) in the cases of CNE/CNA via the dynamics of data flow. Visiting an Internet website, if successful, to evoke an usual case, has invariably for consequence copying and/or deletion of data (both in the form of instructions, as well as effective information), no matter if the actor is a civilian, terrorist, or state employee. As for blocking access to data or incapacitating communication networks, as recent cases proved, group actions, via high volume of requests, overwhelm (DDOS) the response capabilities of transit systems and networks. A single visitor of a website has a modest impact when compared to that of a group. Each visit uses a certain percentage of the processing and communication capabilities of the system, and thus, proportionally to the number of visits, capabilities are reduced up to the point of saturation. In both cases intention (or its absence) is a matter of judicial investigation, not tactical military evaluation.

Risk society

The lexical field pertaining to the concept of security (risk, threat, vulnerability, exploitation, impact, severity, attack, defense, war, criticality), in the context of talks regarding recent international relations and especially

the school of security, and cyberspace security, raised the awareness of all international organizations, of supranational institutions, governments, political and military representatives, civil society, and individuals.

The security concept „patented" by the School of Copenhagen accurately explains the perspective used in the discourse technique addressing objects to be secured by a subject. The existence of security is conditioned by a threat, by the necessary existence of a threatening, harmful agent. Where its existence cannot be demonstrated, it can be speculated.

In order to be effective, security must identify an object finding itself under existential threat. The threat can be anything in the category of what is possible (not probable). Since anything is possible, it does not contradict socially accepted norms (in order to avoid ridicule, few social or political actors engage in pseudoscientific discourse or speculation, and they do it rarely) or it has a minimally calculated probability (it is negligible). In the security process, previously accepted rules can be bypassed. Saving the object is of primordial importance.

In order to produce effects, the importance of the object or the criticality level, the severity of the direct or facilitated threat must be accepted by the audience. The threat is not formulated towards the object itself, but towards life or the fundamental values of societies.

The necessity of security is not oriented towards cyberspace, but towards society. The threats exploit vulnerabilities existing in cyberspace (or in functions facilitated by cyberspace) because they pose a risk to human life or societal values. The criticality of the object (life or fundamental values) amplifies the severity of the threat, imposing the most drastic measures to remove the threat. An answer sizing up to the threat can only be given by the iron arm of society: military institutions, the only ones capable to decisively respond to radical threats on life or fundamental values. In the fight or war between the agent of the diffuse, imprecise, but critical threat, and the armed forces, any sacrifice is acceptable. In order to save life and values not even life itself is too much to sacrifice.

Alongside democracy, freedom of expression, knowledge and emancipation, terror as well propagates (at seemingly even greater speed) through cyberspace. Democracy itself becomes a dictatorship, freedom of expression becomes terrorist propaganda, knowledge becomes weapon

making and destructive knowledge, and emancipation becomes primitive hatred.

Although it is easy to compare pre-Internet technologies to contemporary ones, and their extreme effects, the cyberspace facilitates the most subversive discourses. The printing press challenged the supremacy of religious institutions and of delirious societies, the radio facilitated the transfer of Nazi hatred and Communist propaganda to an even greater extent, and nonetheless it is not looked upon worryingly in any society, television immortalized the most shocking human actions, but it remains desirable as a social function even though it presents the marginal phenomena of human behavior.

The critique of the concept of cyber power

The concept of cyber power refers to a government's exercise of the threat to launch cyber attacks on another country. The unit of measure for cyber power seems to be in this case the credibility of a threat, launched by a government, to engage in cyber attacks. The closer it is to being certain, the more prominent its character of cyber power. By being quite diffuse, this concept deprives the reader of the correlation between the certainty of a commitment and the capacity to carry out the threat with considerable impact. The mere intention, or engaging in the threat of a cyber attack does not itself represent a risk factor, as it represents a measuring unit for (im)morality. In this case, lack of power is highlighted.

Cyber power, by NATO methods, is exclusively used outside war theaters. The total commitment in the case of kinetic conflict is a truism. In the case of military engagement, the cyberspace is a component of the war theater, being, alongside psyops and propaganda, an attribute of secondary, support units. Cyber power and associated components, cyber warfare and cyber espionage, characterize exclusively the periods of military disengagement - peacetime. The army thus manages, at least on a discourse level, to ensure a permanent state of war, at least as seen by its personnel.

The problem of security, in NATO's perspective, becomes corrosive when it is applied to civilian models in periods of military disengagement. In the context of military engagement, the security of communication networks is one of last components of the risk facing the aggressor or the aggressed. In kinetic intervention, communication networks become

security components. In periods of disengagement they are components to be secured.

The reasons for accelerating security can only be speculated upon: from substantially increased budgets to respond to assumed cyberspace engagements to the intrigue unraveled by the possibility of exploring a new environment for the study of conflicts, from political capital gain by private corporations invested in the field to civil society charmed by the idea of absolute order, from enriching the vocabulary of political rhetoric to political gains.

The concept of cyber power includes another term that is common to military thinking: cyber weapons. It is actually a reconceptualization of the term „exploit", or the technique of exploiting a vulnerability, defined as software which addresses one or several defects (vulnerabilities) in order to introduce an execution code whose effects are chosen by the attacker within the limits imposed by the context of the identified vulnerability.

Applying security

The security paradigm of cyberspace includes and relies exclusively on the model being used to define the context and supposed intention of the enemy. In the case of cyber espionage, as well as cyber terrorism - dichotomic models centered on effects - it is not the intention of the enemy, or the lack of protection mechanisms, that exposes possible tactics of exploiting system vulnerabilities. The military defense model used to consist in isolation, segregation, and control. Their absence is to be compensated by isolating individuals, segregating transportation environments, and controlling information nation-wide. Precisely that which Internet connection does not offer, since the purpose of communication is disseminating knowledge, facilitating access to information, and the ability to use them to advance one's purposes. The worries generated by lack of control are an effect of professional (military) nature, since exaggerating risks is preferred to their underestimation in case of failure, for fear of being accused of incompetence.

Security depends on the level of control exercised on the object. For adequate protection it is necessary to adequately control context. In a context of apocalyptic threats, total control is required.

Models for controlling information transfer had started to appear since the 90's (at the same time as the invention of HTML and the development of electronic mail), when agencies such as CGHQ or the NSA were soliciting copies of encryption keys (in order to decipher messages) when certain advanced encryption forms were used (practically, anything that would have delayed decryption processes).

Another initiative followed which took the form of anti-pornography (especially child pornography) campaigns, when, using lack of tolerance for the online presence of such material as a moral pretense, governments were willing to censor information transfer entirely in their attempt to eliminate completely the transfer of offensive data (pornography).

In 2010, two initiatives aiming at information control were discussed in the EU Parliament: ACTA (Anti-Counterfeiting Trade Agreement), aiming to identify and eliminate counterfeit material (piracy), which, by means of generous definitions of the terms in use, could punish almost any kind of information transfer; and Gallo, which runs in tandem with and completes ACTA and addresses exchange of goods for which there is no copyright but which are seen as counterfeit nonetheless. The same generosity in term usage renders the necessity to control information transfer via the Internet mandatory.

Perhaps the most radical measure aiming at information control is filtering and recording communication data and, possibly, the content of communication. By the means of the same generosity of definition and ambiguity of the terms in use, means of control of information dissemination similar to censorship practiced by totalitarian regimes is instituted.

When looking at the conditions imposed on information transfer via the Internet in the People's Republic of China, as well as the consequences of exclusive state control over the dissemination of information and content, the initiatives of the EU and the US in the same direction seem difficult to understand and explain.

The pressures that governments are facing are exerted particularly by the private economic sector, which announces terrible losses because of what they termed as „piracy" (despite the fact that information cannot be stolen, but only copied, as the source remains intact). Media producers (film/music) announce via viral spots the equivalence of data transfer and

theft, expecting regulation, by popularizing the theme of patented data transfer on one hand, and preparing legislation terms and avoiding an unfriendly image amongst consumers, on the other hand.

In a 2009 interview, Cambridge professor Ross Anderson, a specialist in information security, declined the legitimate possibility of controlling information in Western societies, putting forth as arguments the denseness of infrastructure and the amount of information, which would be impossible to control entirely. While from a technical perspective a global control of Internet, military or civilian, is impossible, the pressure to restrict access and exchange of information remains in place. If interconnection paradigms multiply, the arguments for control will be made from a security perspective.

Former Google CEO, Eric Schmidt, advisor in the Obama administration, warns in an article in Foreign Affairs („The Digital Disruption", p. 75, November/December 2010) that „masses of citizens armed with nothing else than mobile phones, organizing mini-rebellions and contesting state authority" will generate surprises in the 21st century. Moreover, Schmidt is confident in the capacity for „great connecting powers such as the USA, EU and Asian countries to regulate interconnection status within their own borders in a way that would strengthen their values", while not hiding his regrets that, in the case of developing societies, where regulation is not possible, there are „new methods for constraint oriented towards political opposition, which makes them closed and repressive societies". When discussing the problem of national security, he warns about the challenges facing the USA and the EU in the context of the expansion of values promoted by countries like China: control and censorship. The image we have in „Digital Disruption" is that governments are the only actors not invited to the round table represented by the Internet. The Richelieu-inspired power game does not find its place in a world connected to an environment which does not accept censorship.

The end-to-end functioning of Internet is that which makes, technically, extremely difficult to control information or enforce censorship, if not impossible altogether. This manner of functioning requires the existence of a center or transfer core lacking the ability to interpret information and leaving the interpretation applications to the model's periphery. This transfer core is transited from one end to the other. On the

ends there are applications for interpretation. For lack of data processing in the core, censorship can only be practiced on the periphery. In the case of China, censorship is applied to search engines (especially Google), that is at the peripheral level, at the end which solicits information (via filtering applications, individually installed on every interconnected computer) or the end that provides the information via regular controls and frames or via installing information transfer brokers (proxy solutions) which respect the end-to-end model controlled by government entities.

Be it civil or military control, the interface control model is to be discussed. As such, terms related to cyber power (cyber warfare, cyber terrorism, and cyber espionage) address the consequences generated by the systems' state of insecurity (or vulnerability). In the case of cyber warfare, control over data transfer by individually interconnected users is exercised via regulations oriented towards communication companies (data storage and data recording). In the case of cyber terrorism control is oriented towards peripheral systems offering information, by using the argument of extremist „propaganda centers", on one hand, and towards entities providing infrastructure services (electricity, gas, etc.) and are connected to the Internet for various reasons, on the other hand. In the case of cyber espionage, control is practiced on state actors and private corporations, namely to the periphery providing information.

There are, undoubtedly, tensions between interconnected actors (individuals, groups, or governments), as well as examples of such cases. The case of Estonia (2007) is well-known: the activities of government institutions and private corporations were blocked following excessive data traffic. The context which facilitated the incapacitation of communication was one of inadequate implementation and existing resilience components. The same scenario that was applied to Estonia, when oriented towards an experienced interconnected entity (Microsoft or BBC, for example), would not have included infrastructure resilience. It is a frequently-cited example, but the risk level is contextual. The case of Estonia is, for all practical purposes, atypical.

BIBLIOGRAPHY

CLARK, R. A. (2010). *Cyber War: The Next* Threat to Naţional Security and What to Do About It.

Distributed Denial of Service

Ecco Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, California, USA: Rand Corporation

European Network and Information Security Agency

http://daccess-dds ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?

http://en.wikipedia.org/wiki/United_States_Cyber_Command

http://www.bbc.co.uk/blogs/digitalrevolution/2009/11/rushes-sequences-ross-anderson.shtml

http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf

http://www.guardsmark.com/files/computer_security/TLR_Oct_10.pdf

http://www.laquadrature.net/en/dossiers

http://www.nato.int/cps/en/natolive/official_texts_68580.htm#cyber

http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf

http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf

Rice, D. (2008). *Geekonomics. The real cost of insecure software. Addison-Wesley*

National Security Agency

UK Government Communications Headquarters

United States Cyber Command

United States Department of Defense