UNIVERSIDADE CATÓLICA PORTUGUESA

Cyber Warfare
in the context of International Criminal Law

Rafaela Macedo de Figueiredo Carvalho Miranda

Faculdade de Direito | Escola do Porto

2016

UNIVERSIDADE CATÓLICA PORTUGUESA

Cyber Warfare
in the context of International Criminal Law

Rafaela Macedo de Figueiredo Carvalho Miranda

Faculdade de Direito | Escola do Porto

2016

It is with a deep sense of gratitude and honor
that I dedicate this Master Dissertation to my parents and my brother.

É com imensa gratidão e honra
que dedico a presente Dissertação de Mestrado aos meus pais e irmão.

Acknowledgments

I will never be able to thank my parents and brother to the extent they truly deserve, but I will try – *Thank you* for being the role models I proudly look up to; for teaching me strong values, morals and principles that allow me to stand up for myself without disrespecting others; for making me forget about the distances, by being so present and following every single step of mine; for motivating me to accomplish more, do better and go further… I will continue to do my best, but that is only possible with you by my side!

To my teacher and mentor, Dr. Nuno Pinheiro Torres, *thank you* for believing I had the skills needed to address such a complex topic and for encouraging me to respond to the high expectations you set for me. But, more importantly, thank you for the patience, consideration and interest demonstrated throughout this process.

I would like to *thank* Mr. Christian Lifländer, Mr. Rogério Raposo and Mr. Tomáš Minárik for the willingness and courtesy in providing me the opportunity to conduct such enlightening interviews about the subject of my Master Dissertation.

Thank you, NATO Cooperative Cyber Defence Centre of Excellence – in the person of the Director Sven Sakkov – for authorizing my visit to the CCD COE facilities located in Tallinn and for kindly managing time to meet me in person and to know more about the outcomes of my Master Dissertation.

All of you directly supported me in the achievement of a very important objective in my personal and professional life and, for that, I will be forever grateful.

Obrigada!

Abstract

The conceptions of warfare and battlefield have astonishingly evolved, going from a traditional view of military ammunition performed in land, sea or air, to the most novel electronic devices which rule today's international conflict strategies in cyberspace. Some examples of the latter weapons operating in the so-called fifth domain, like pen drives, drone strikes, keyboards and malware, are even considered innocuous at the first glimpse, especially when compared to other type of classic artillery. Howbeit, these gadgets were the ones that fostered the current limitless cyber race – which was noticeably triggered by the cyber attack occurred in Estonia (2007) – and has since then proved capable of causing way more alarming consequences, mainly if targeting critical national infrastructures. This present dissertation will dwell on the analysis of the enforcement of international law bodies towards acts of cyber war carried out by state or non-state agents, taking into specific consideration the application of the international criminal law norms. Thereunder, the focus of the study will remain on the characterization of cyber attacks, as either potential crimes of war or aggression.

Keywords: cyberspace; cyber war; cyber attacks; international criminal law; crime of aggression; crime of war.

Table of Contents

Acronyms

ATM – Automatic Teller Machine

CCD COE - Cooperative Cyber Defence Centre of Excellence

CNI – Critical National Infrastructure(s)

CoE – Centre of Excellence

DDoS – Distributed Denial of Service

DNC - Democratic National Committee of the United States Democratic Party

ECIs – European Critical Infrastructures

FBI – Federal Bureau of Investigation

GPS – Global Positioning System

ICC – International Criminal Court

ICJ – International Court of Justice

ICL – International Criminal Law

ICTY – International Criminal Tribunal for the Former Yugoslavia

IHL – International Humanitarian Law

NATO – North Atlantic Treaty Organization

NIST - National Institute of Standards and Technology of the United State's Department of Commerce

NSA – National Security Agency

OPM - United State's Office of Personnel Management

OSCE – Organization for Security and Co-operation in Europe

SCADA - Supervisory Control and Data Acquisition

UN – United Nations

Introduction

The twenty-first century is undoubtedly the era of fast and massive proliferation of technology, being the unhindered access of internet the ultimate power relying on the fingertips of any human being. This continuous evolution of the cyber world makes it simultaneously appealing and hazardous, because there is a whole range of tools and online information easily available to everyone eager to get it, irrespective of the user's gender, age, nationality, job or intent. With the new millennium highly praised electronic characteristics, like omnipresence and anonymity, some inevitable consequences came along, such as lack of oversight and traceability difficulties. So, it is not surprising that notions like cyber warfare, cyber terrorism or cyber attacks are now intrinsic part of the present lexicon of political leaders, high representatives of international organizations and legal experts.

Therefore, and since law has to follow up society's transformation and earnestly reflect it in order not to become obsolete, international law needs to face this growing transnational cyber phenomenon and set a feasible universal framework. Unfortunately, very few meaningful efforts are being made in order to overcome the ambiguity of cyber conceptions and lack of legal harmonization, and ultimately, to achieve a contemporary, unanimous and comprehensive legal regime for cyberspace. This inertia can be ascribed to diverse factors – the novelty and uniqueness of the topic; the political clout of States that are in the forefront of cyber development and are keen to use it as a military asset; the inaudible protest of nations that are victims of cyber attacks, mostly because of their interest in camouflaging national security breaches; and finally, the existence of international law, *viz.* law of war, that may render a creation of a specific legal body for cyberspace unnecessary. Nevertheless, the Tallinn Manual on the International Law Applicable to Cyber Warfare[1] took a promising first step towards the right direction, as it constitutes "(…) an attempt to absorb the uncertainties surrounding cyberwar through legal reasoning and the application of rules (…)"[2]. The Tallinn Manual's process was promoted by NATO, more specifically by the Cooperative Cyber Defence Centre of Excellence, with the aim of addressing relevant topics pertaining the cyberspace spectrum. A group of high profile legal and technical experts, directed by Michael N.

[1] Full text is available at www.ccdcoe.org/tallinn-manual.html [accessed 2 September 2016]

[2] Kessler, O. & Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26, 797.

Schmitt, conducted a three year project that culminated in a set of ninety-five rules with corresponding commentaries that expressed the group's open discussion about its interpretation and applicability. Although the Tallinn Manual was not intended to outline an official position on cyber conflicts, it surely is not an overstatement to define it as a milestone. No other collective document, neither before or after its publication in 2013, ventured to insightfully analyze the piecemeal collection of international norms on a cyber standpoint. Thereunder, the Tallinn Manual "(…) is an influential document toward that end, and it has been treated as such. It did not create new law, nor suggest possible international agreements that might be adopted. It did create consensus, non-binding document that could form the basis for future negotiations"[3].

The conundrum of cyberspace and the focal point of this dissertation is the recognition of which international principles, norms and rules apply to cyber attacks. Accordingly, we will focus on the importance of advocating international cooperation in furtherance of consensus and legal clarity in the cyber context, most importantly in terms of accountability of aggressive actors. Needless to say, online threats can emerge either from States or non-State organizations, and since we are currently facing an ominous surge of terrorist attacks worldwide, the presence of the last group in the cyber domain has increased significantly. "Non-State actors continue to grow in importance, gaining the skill and the expertise necessary to wage asymmetric warfare using non-traditional weaponry that can create devastating real-world consequences"[4]. Even though attributing the attack to its real agent can be frankly intricate, "The International Criminal Court—the only criminal tribunal in the world with global reach—holds significant promise in addressing this threat"[5]. In spite of the public acknowledgment of the occurrence of cyber attacks in some countries and of the undeniable involvement of many others in these type of operations, up until now no concrete sanction was observed nor any international court was implicated in cyberspace. Perhaps the apparent absence of international legal effects is due to the lack of severe impact and humanitarian nefarious consequences of the past cyber attacks. In reality, the general society still immediately associates cyber conflict with events akin to WikiLeaks or Anonymous, disregarding at the outset the possibility of cyber weapons shutting down power grids, deregulating dams or disconnecting traffic

[3] Chayes, A. (2015) Rethinking Warfare: The Ambiguity of Cyber Attacks. *Harvard National Security Journal*, Vol.6, 501

[4] Ophardt, J. (2010) Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review*, Nº3, Abstract

[5] *Ibid.*

lights, for example. The large scepticism concerning the feasibility of deaths and physical havoc as an expected result of cyber warfare makes even more urgent the necessity of debating the regulation of cyberspace and enhancing public perception on eventual outcomes. As a matter of fact, every scenario is possible in cyberspace – from financial losses as a result of an attack to the stock exchange, up to human damages caused by intentionally switching off the public emergency telephone lines.

I. Conceptual Framework

Antagonistically to physical space, cyberspace can be vaguely described as the realm of the immeasurable, ubiquitous and intangible. This illustrative triad shows how challenging can be the apperception of the online reality and the scrutiny of cyber events. However, the society is inevitably becoming more and more aware of the pros and cons of the virtual world, all because of the globalization and the consequential general dependency on information systems and network access. "Today, states, non-state communities, business, academia and individuals have become interconnected and interdependent to a point never imaginable before"[6]. So, we can proudly say we are part of a global village, but we also have to bear in mind that this wellspring brings more vulnerability towards crime and conflict. In this regard, cyberspace can be defined as an extension of human capacities into a limitless platform of communication, where real scenarios are virtually represented and are not subjected to geographical boundaries. Informatics tools allow users to anonymously share data or information in a multilevel dimension, converting cyberspace into "(…) the only domain which is entirely man-made"[7]. It is relevant to note that cyberspace is not merely composed by internet, as it involves other type of technologies and telematics, such as GPS, clouds or digital sensors.

Some countries with conventional military superiority see the loom of cyberspace as a wakeup call to the need of developing innovative warfare techniques and strategies. Many authors[8] expressed concerns about the possibility of a "Digital Pearl Harbor"

[6] Melzer, N. (2011) Cyberwarfare and International Law. *UNIDIR Resources*, *Ideas for Peace and Security*, 3

[7] *Ibid.*, 5

[8] *Cf.* Nunes, P. (2004) Ciberterrorismo: Aspectos de Segurança [Cyberterrorism: Security Aspects]. *Revista Militar*, Nº 2433, 1; Kessler, O. & Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26, 801

scenario in the future; Admiral Michael Rogers, Director of the National Security Agency of the United States of America, confirmed that theory by claiming that it is only a matter of time for a mega cyber attack to happen[9]. In spite of the lack of unanimity regarding cyber definitions, it is valid to state that the distinction between a cyber operation and a cyber attack underlies on the impact of the act itself, the level of damages and the ability of the victimized State to restore the public order and safety. A cyber operation consists in the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace"[10]. On the other hand, "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[11]. It is noticeable that the difference between the two concepts lies on the purpose of the action and expectations raised on the consequences that may arise from it. Some academics[12] propose the addition of a political or national security finality to the definition of cyber attack, classifying the ones that are not conducted with that specific purpose as cyber crimes. In order to justify that assertion, two arguments are invoked – first, non-political cyber operations "(…) do not raise the same legal questions as activities that might breach public international law. (…) Second, a cleaner delineation between cyber-attacks that present threats to national security and purely private cyber-crime will clarify ownership of cyber-security needs among various government departments"[13]. We do not share the aforementioned point of view, on the grounds that cyber crimes encompass a wide range of illegal activities in cyberspace (e.g. phishing scam, fraud, distribution of online child pornography, intellectual property infringement and online harassment). Besides, cyber attacks are expected to undermine the target, whereas cyber crimes do not necessarily seek that. Moreover, the resort to a political purpose precondition should only be observed in the context of cyber war and cyber terrorism, the latter being described as the perpetration of a cyber attack with the intent of intimidating or compelling a State government and resulting in such human or physical violence capable of instigating general fear. Hence, cyber attacks are imperatively cyber crimes – with the exception of launching a cyber attack within the

[9] Adm. Michael Rogers on the Prospect of a Digital Pearl Harbor. (2015, October 26) *The Washington Post*. Retrieved from http://www.wsj.com/articles/adm-michael-rogers-on-the-prospect-of-a-digital-pearl-harbor-1445911336 [accessed 17 September 2016]

[10] Tallinn Manual, 258

[11] Tallinn Manual, Rule 30, 106

[12] *Cf.* Hathaway, O. & Crootof, R. (2012) The Law of Cyber-Attack. *Yale Law School Legal Scholarship Repository*, *Faculty Scholarship Series*, Paper 3852, 821

[13] *Ibid.*, 831

right of self-defense – but not all cyber crimes rise to the level of a cyber attack. As will be explained below, cyber attacks can be promoted by States or non-State actors, like terrorist cells, criminal organizations or affiliated groups. Nonetheless, only cyber attacks conducted by States and with repercussions tantamount to conventional kinetic armed attacks or taking place in the context of an armed conflict lead to a cyber warfare.

"Attacks can rapidly go global (…) with the result that many nations are quickly drawn in. And it is in this context that the term 'cyberwar' has become a frequently used buzzword to refer to any kind of conflict in cyberspace with an international dimension. Such a broad use of the term, however, is not helpful (…)"[14]. Indeed, "Arguing the semantics of the term «cyberwar» is, itself, a war of words. There is no legal definition of the term"[15]. Not even Tallinn Manual's international group of experts was able to provide a consensual definition of it, but still made it clear that "(…) the fact that States lack definite guidance on the subject does not relieve them of their obligation to comply with applicable international law in their cyber operations"[16]. In this context, it is important to assert that we do not see any advantage in multiplying misconceptions, especially since it believes war can assume different shapes, being cyber ineluctably one of the numerous types of conducting a conflict. The world is changing, so is the philosophy of war. Therefore, it is time to acknowledge that new strategies, tactics and weapons emerge every day and even though interrelating them with traditional definitions widely accepted for years by academics is very challenging, that is an exercise we simply cannot dismiss. Ergo, it can be assumed that cyber warfare stems from hostile cyber attacks that are launched within the scenario of armed conflict or unleash the same kinetic effects as the ones provoked by conventional weapons. Since we are dealing with a typology of war is also required the existence of a political agenda or an undeniable intent of thwarting the normal functioning of the victimized State. "The notion that an information-age would be bloodless and sterile is challenged by the fact that our digital infrastructures and physical capabilities are integrated in order to sustain and support modern warfare"[17]. Information is the key enabler of cyber war, so much that when we

[14] Schreier, F. (2015) On Cyberwarfare. *DCAF Horizon*, Working Paper Nº7, 7

[15] Brownlee, L. (2015, July 16) Why 'Cyberwar' Is So Hard To Define. *Forbes*. Retrieved from http://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/1/#664ba43c2eaa [accessed 2 September 2016]

[16] Tallinn Manual, 3

[17] Colarik, A. & Janczewski, L. (2012) Establishing Cyber Warfare Doctrine. *Journal of Strategic Security*, Volume 5, Nº1, Article 7, 39

discuss cyberspace we cannot sideline the influence of information networks as simultaneously targets and tools of cyber attacks (block access to communication systems or use data streams to destroy an infrastructure, respectively). “Over the last decade, military thinkers have devised and developed a term – information operations – anticipating this «new category of warfare» that grows from the Internet’s interconnectivity and other new forms of communication”[18]. As in cyber definitions, “(…) the term «information warfare» is often inaccurately used as a synonym for «information operations»: while the latter can occur both in times of peace and war, the former refers exclusively to information operations conducted in situations of armed conflict and excludes information operations occurring during peacetime”[19]. In turn, “Information warfare covers a much broader range of activity than computer networks attacks, however. It also includes psychological operations and perception management, deception, electronic warfare and intelligence collection”[20].

II. *Jus ad Bellum*

Considering that *jus ad bellum* establishes when nations can legally engage in war, apparently there is no doubt this is the set of criteria which countries have to comply with if they purport to partake in a conflict. “In *jus ad bellum* analyses, the notion of «use of force» is often confused that of «armed attack»”. The former bears on whether an action violates international law as codified in Article 2(4). By contrast, act(s) that cross the armed attack threshold found in Article 51 of the U.N. Charter (and customary international law) concern a target-state’s entitlement to respond defensively with its own kinetic or cyber use of force”[21]. In respect of every nation’s territory, sovereignty and independence, Article 2 nº4 of the United Nations Charter sets the provision that bans the use of force by States, which means only non-State organizations’ cyber attacks that are amenable to be attributed to a State are covered by this general rule. However, there are two lawful exceptions to this prohibition, *i.e.* authorizations of use of force by the Security

[18] Hollis, D. (2007) Why States need an International Law for Information Operations. *Lewis & Clark Law Review*, Vol.11:4, 1028-1029

[19] Melzer, N. (2011) Cyberwarfare and International Law. *UNIDIR Resources*, *Ideas for Peace and Security*, 22

[20] Denning, D. (2001) Obstacles and Option for Cyber Arms Controls. *Georgetown University*, 6

[21] Schmitt, M. (2012) International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, Volume 54, 18

Council, in compliance with Article 42 of the UN Charter, and the right of self-defense, enshrined in Article 51 of the same document.

The Article 39 of the UN Charter accredits the Security Council to identify threats to peace or acts of aggression, and consequently, to restore the international security by making recommendations or deciding to take non-forceful or forceful measures, correspondingly set forth by Articles 41 and 42. Resort to violence and use of armed force would unquestionably activate the authorization of the Security Council; but, in what grounds is this assessment conducted in the cyber realm? Whereas cyber operations wreaking dramatic physical and human damages would most likely qualify, others spawning different (yet significant) consequences would remain dubious. The ICTY elaborated on the subject, in the Tadić case, concluding that "(…) While the «act of aggression» is more amenable to a legal determination, the «threat to the peace» is more of a political concept. But the determination that there exists such a threat is not a totally unfettered discretion, as it has to remain, at the very least, within the limits of the Purposes and Principles of the Charter"[22]. Despite of this assertion, reality shows there is no mechanism, body or institution responsible for reviewing Security Council's authorizations. "This being so, the Council may label any cyber operation a threat to the peace (or breach of peace or act of aggression), no matter how insignificant"[23]. Moreover, the use of force granted by Article 42 of the UN Charter, when literally read, does not include actions in cyberspace but only those taken by air, sea or land. However, we can deduce that San Francisco Conference delegates[24] did not have, at the time, any plausible reason to exclude the fifth domain from the UN Charter's draft, simply because waging war in cyberspace was still inconceivable[25]. Consequently, we align with a purposive interpretation of the UN Charter and firmly believe Security Council should also comprise cyber operations in its authorizations, in order to fully guarantee the re-establishment of

[22] *Prosecutor v. Dusko Tadić (Decision on the Defence Motion For Interlocutory Appeal on Jurisdiction)*, IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995, §29.

[23] Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, *The National Academies Press*, 161

[24] The San Francisco Conference took place in 1945 and assigned the UN Charter's drafting to the heads of delegations that were appropriately grouped in a Steering Committee, an Executive Committee and a Commission. More information about the process of preparation of the UN Charter available here: http://www.un.org/en/sections/history-united-nations-charter/1945-san-francisco-conference/index.html [accessed 29 August 2016]

[25] Natário, R. (2016) O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço [Combat against Cybercrime: Anarchy and Order in Cyberspace]. *Revista Militar*, Nº2541, 3

international peace and security. “Finally, it must be recalled that the entire UN collective security system depends on the readiness of the five Permanent Members of the Security Council (P5) to allow for action by refraining from exercise of their veto right”[26]. It is quite naive to consider that China, Russia or the United States of America would not take advantage of this power, especially knowing the amplitude of their investment in developing cyber capabilities.

The second exception to the prohibition of the Article 2 nº4 is the inherent right of states to defend themselves; *vis à vis*, “(…) while the use of force prohibition only applies to the acts of states (or those attributable to states under the law of state responsibility), the right of self-defense arguably encompasses attacks mounted by nonstate actors”[27]. Since Article 51 of the UN Charter exclusively admits self-defense as a response to armed attacks[28], it is essential to shed light on its outlines. In the Nicaragua case, the ICJ drawn a distinction between armed attack and use of force predicated on the “(…) scale and effects (…)”[29], implying the resort to use of force is “(…) less grave, not amounting to armed attack”[30]. This decision left lots of room to skewed interpretations of the armed attack threshold, mainly because no specific criteria was set by the Court. In a subsequent case, the ICJ even acknowledged the possibility of “(…) the mining of a single military vessel might be sufficient to bring into play the «inherent right of self-defence»”[31], which indicts “(…) qualitative indicators of attack (death, injury, damage or destruction) are more reliable in identifying those actions likely to be characterized as an armed attack than quantitative ones (number of deaths or extent of destruction). So long as cyber

[26] *Ibid.*, 162

[27] Schmitt, M. (2012) International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, Volume 54, 18

[28] Regardless, there are still countries that publicly recognize “(…) that the inherent right of self-defense potentially applies against any illegal use of force” Koh Speech delivered during the USCYBERCOM Inter-Agency Legal Conference, Part I. Question 1. Retrieved from http://www.state.gov/s/l/releases/remarks/197924.htm [accessed 4 September 2016]. On 18th September 2012, Harold Koh, Legal Adviser of the United States’ Department of State, made some remarks on the country’s stand on the application of international law to cyberspace. To summarize, the United States of America decided to swim against the tide by attesting that the right of self-defense is not only triggered by armed attacks, but also by imminent threats. These statements are in compliance with the United States’ manifest intention of responding to hostile acts in cyberspace in the same manner as they would do in any other domain.

[29] Military and Paramilitary Activities in and against Nicaragua *(Nicaragua v. United States of America)*, Judgement, International Court of Justice (ICJ), 27 June 1986, §189.

[30] *Ibid.*, §210

[31] Oil Platforms (*Islamic Republic of Iran v. United States of America*), Summary of the Judgement, International Court of Justice (ICJ), 6 November 2003, §72

operation is likely to result in the requisite consequences, it is an armed attack"[32]. The Tallinn Manual's experts put it plainly by affirming "(…) some cyber actions are undeniably not uses of force, uses of force need not involve a State's direct use of armed force and all armed attacks are uses of force"[33]. Their endeavor took a step further with the articulation of a consensual but non-exhaustive list[34] of eight characteristics that cyber operations should comprise in order to be regarded as uses of force. *Severity* is by far the most important factor of the cluster, particularly because it comprises the scope, duration and intensity of the cyber operation. The consequences of the attack need to go beyond the mere inconvenience or annoyance and reach a severe level of damages, whether physical or human. The destruction of critical national infrastructures and the injury or death of individuals will obviously amount to a use of force; on the contrary, economic or political coercion[35], acts of espionage[36], psychological cyber operations[37] and providing financial support to a rebel's group[38] will almost certainly not[39]. The destruction of intellectual property, data or other intangible resources may be considered uses of force, but would not suffice to constitute armed attacks, unless it indirectly lead

[32] Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, *The National Academies Press*, 164

[33] Tallinn Manual, 47-48

[34] Tallinn Manual, Rule 11 nº9

[35] Tallinn Manual, Rules 10 nº10 and 11 nº2 and nº9 h); "The Charter's *travaux préparatoires*, indicate that during the drafting of the instrument a proposal to extend the reach of Article 2(4) to economic coercion was decisively defeated. A quarter century later, the issue again arose during proceeding leading to the UN General Assembly's Declaration on Friendly Relations. (…) Whatever force is, then, it is not economic or political pressure. Therefore, a cyber operation that involves such coercion is definitely not a prohibited use of force" Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, *The National Academies Press*, 155

[36] Tallinn Manual, Rule 11 nº9 h), 30 nº2 *in fine* and 66; "Espionage is not considered to be an act of war or aggression, and computer espionage should be similarly regarded" Denning, D. (2001) Obstacles and Option for Cyber Arms Controls. *Georgetown University*, 8; "(…) there is no international law prohibiting espionage or insisting it violates sovereignty. (…) As cyber activities are frequently akin to espionage, even if conducted for another purpose, perhaps it is not too much of a leap to assert that most cyber activities can also occur without violating territorial sovereignty" Brown, G. & Poellet, K. (2012) The Customary International Law of Cyberspace, *Strategic Studies Quarterly*, *US Cyber Command*, *Fort Meade*, 20755, 133-134

[37] Tallinn Manual, Rules 11 nº3, 11 nº9 h), 30 nº2 *in fine*, 31 nº5 and 61 nº2 f); "Psychological Operations (PSYOP) are planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups and individuals" Schreier, F. (2015) On Cyberwarfare. *DCAF Horizon*, Working Paper Nº7, 20; For illustrative purposes only – false flag acts, broadcasting false statements as official ones, dissemination of political propaganda or sponsoring demoralization can constitute PYSOP.

[38] "(…) it does not consider that military maneuvers held by the United States near the Nicaraguan borders, or the supply of funds to the *contras,* amounts to a use of force." Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), Judgement, International Court of Justice (ICJ), 27 June 1986, §228.; Tallinn Manual Rule 11 nº3.

[39] Tallinn Manual, Rule 11 nº9 h)

to substantive material damages[40]. Even so, "The fact that a cyber operation does not rise to the level of a use of force does not necessarily render it lawful under international law. In particular, a cyber operation may constitute a violation of the prohibition on intervention"[41]. *Immediacy* is the temporal factor, which implies that the longer cyber operation's impact takes to be noticed, the less chances there are for it to be considered use of force, because the victimized State has more time to fend off and mitigate its negative effects. *Directness* focus on the existence of a causal link between the attack and its effects. It is easier to identify uses of force when the connection is direct (for instance, urban flooding as a result of a cyber attack that opens a dam), but not so much when it is indirect (for example, a cyber attack targeting the patients' database system of a hospital could lead to the death of a penicillin-allergic person, because paramedics would not have electronic access to those type of information). *Invasiveness* refers to the level of intrusion managed by the attacker into the victim's vulnerabilities; hence, successful cyber attacks in military or highly secure national systems are more likely to be sorted as uses of force. The *measurability of effects* predicates the qualitative estimation of losses produced. If the majority of damages is material, it is less challenging to identify the extent of the attack's effects. A cyber attack with undetermined consequences is more difficult to measure and the probability of it being equated with a use of force will be smaller. Regarding the factors of *military character* and *state involvement*, once the operation directly victimizes or derives from the military or a nation there is a high likelihood for it to be considered use of force. Lastly, the *presumptive legality* relates to the dictum that everything that is not forbidden by international law is, in general, accepted and therefore cannot be deemed use of force.

Before concluding, it is fundamental to address a pivotal question – can non-destructive cyber attacks be reckoned as armed attacks? Alas, "The International Group of Experts could achieve no consensus as to whether such activities amounted to sovereignty violations. Arguably, the distinction between cyber operations resulting in physical damage or injury and those that do not is overly formalistic. (…) The prohibition

[40] "(…) the destruction of or damage to the data would have to result in physical consequences, as in causing a generator to overheat and catch fire or rendering a train or subway uncontrollable such that it crashed. (…) banking data, could also be reasonably encompassed within the scope of «armed attacks»". Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, *The National Academies Press*, 164

[41] Tallinn Manual, Rule 10 nº6

on intervention, which requires coercive intent but not physical damage or injury, illustrates, it would seem, the lack of an all-encompassing requirement for physical effects"[42]. Even though for countries like the USA, the verification of an overall physical damage is primary for this type of assessment[43], that does not prevent it from publicly acknowledging that "(…) there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions (…)"[44]. In Nicaragua, the ICJ opened a very promising window of opportunity by declaring that "(…) the United States has committed a prima facie violation of the principle by arming and training the *contras* (…)"[45]. In other words, "The ICJ has rejected a narrow interpretation of «use of force» that limits the term to the employment of either kinetic force or non-kinetic operations generating comparable effects. (…) The logic of the holding leads to the conclusion that non-destructive cyber operations can sometimes amount to a use of force"[46]. The Tallinn Manual corroborated the Court's ruling by admitting that giving malware to an organized group and training how to use it would constitute a form of use of force[47]. Nonetheless, this argumentation cannot be immediately presumed as equally viable for the category of armed attacks, because this last concept differs from the use of force. Accordingly, advocating that any cyber operation, regardless of the nature of its effects, could eventually cross the threshold of an armed attack and justify a self-defense response is a bold statement, but we are willing to stand for it. It is our firm belief that whenever a cyber attack targets a country's CNI or armed forces, provoking severe non-destructive or non-injurious consequences, it could correspond to an armed attack. This suggested case-by-case analysis would have to focus on the severity of the consequences, rather than its nature. A properly planned cyber attack against one of these two highly valuable national assets could seriously disrupt the normal functioning of a State as well as compromise the stability of the society for a long period of time. In our opinion, this sort of cyber offensive, albeit not necessarily resulting in physical damage, could justify a

[42] Schmitt, M. (2014) The Law of Cyber Warfare: Quo Vadis?. *Stanford Law & Policy Review*, Vol.25:269, 275

[43] Graham, D. (2010) Cyber Threats and the Law of War, *Journal of National Security Law & Policy*, Vol 4:87, 91

[44] Koh Speech delivered during the USCYBERCOM Inter-Agency Legal Conference, Part II. Question 1. Retrieved from http://www.state.gov/s/l/releases/remarks/197924.htm [accessed 4 September 2016]

[45] Military and Paramilitary Activities in and against Nicaragua (*Nicaragua* v. United States of America), Judgement, International Court of Justice (ICJ), 27 June 1986, §227.

[46] Schmitt, M. (2014) The Law of Cyber Warfare: Quo Vadis?. *Stanford Law & Policy Review*, Vol.25:269, 279-280

[47] Tallinn Manual, Rule 11 nº4

response in self-defense from the victimized country when compromising its ability to carry out vital functions and affecting the public interest. Plus, these attacks are an inevitable public display of the national vulnerabilities of the victim, making other potential aggressive countries immediately infer that if the victimized State was not in a position to prevent a non-physical attack against its most valuable assets, as a matter of logic, it will not be able to prevent a prospective physically destructive cyber operation. It may seem safer to hide behind the argument of the lack of State practice regarding the qualification of non-destructive cyber operations as armed attacks, however this traditional perspective could eventually backlash – "(…) [it] will either end up being too restrictive (that is, including only cyber operations directly resulting in physical destruction but not, for example, the «mere» incapacitation of the entire national power grid, telecommunication network or air defence system) or too expansive (that is, including any large scale denial of service attack even against non-essential, purely civilian service providers such as, for example, online shopping services or telephone directories)"[48]. That being the case, some countries and authors, with whom we are aligning, ventured a different approach. The Netherlands is the prima example of this due to the release of an audacious report on cyber warfare, which declared that "A disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. However, a cyber attack that targets the entire financial system or prevents the government from carrying out essential tasks (…) could well be equated with an armed attack"[49]. Although Tallinn Manual's experts concurred with the idea that armed attacks can have non-kinetic nature[50], they did not reach consensus on which type of weapons conform to the prefix 'armed'. Whilst some were upholders of the traditional interpretation, "[o]thers took the view that it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of ensuing effects"[51], pointing out as an example a deliberated cyber crash of the New York Stock Exchange. Conversely, the same group agreed on the possibility of accumulating multiple severe non-physically

[48] Melzer, N. (2011) Cyberwarfare and International Law. UNIDIR Resources, Ideas for Peace and Security, 14

[49] Dutch Advisory Council on International Affairs and Advisory Committee on Issues Of Public International Law (2011) Cyber Warfare Report, Nº77 AIV/Nº22 CAVV, 21. Retrieved from http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf [accessed 10 September 2016]

[50] Tallinn Manual, Rule 13 nº3

[51] Tallinn Manual, Rule 13 nº9

damaging cyber attacks, derived from the same perpetrator, and considering them as a one sole armed attack[52].

III. *Jus in Bello*

The application of International Humanitarian Law rules will depend on whether the cyber hostility was employed in an armed conflict or not; "(…) in the absence of an armed conflict the protective scope of IHL would not govern the situation. Other bodies of law (…) might, of course, apply and provide their own protection"[53]. Nonetheless disagreement remains among Tallinn Manual's experts on the definition of armed conflict[54], Article 2 of the 1949 Geneva Convention (IV)[55] posits an accurate definition of armed conflict as cases of declared war which may occur between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them, which was already validated by ICTY in the Tadić case[56]. Still, it urges to dwell on the interpretation of armed force and on the dilemma of attribution of cyber attacks, because both are indispensable preconditions to the assessment of the existence of an armed conflict.

There is no universal "(…) meaning of armed force in IHL because it is a jurisprudential criterion"[57] and, *a priori*, the analysis of it may sound as a redundancy, because the concepts of use of force and armed attack were already previously examined. But in fact, "(…) it should be recalled that the objects of regulation of *jus ad bellum* and *jus in bello* are entirely distinct: while *jus ad bellum* specifically regulates inter-state relations and the requirements for the lawful resort to force between states, *jus in bello* regulates the behavior of parties to the conflict (…) This differentiation equally applies

[52] Tallinn Manual, Rule 13º nº8

[53] Droege, C. (2012) Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross,* Vol.94, Nº886, 547

[54] Talinn Manual, Rules 20 nº5 and 21 nº3

[55] relative to the Protection of Civilian Persons in Time of War

[56] "(…) we find that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State." *Prosecutor v. Dusko Tadić (*Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995, §70.

[57] Droege, C. (2012) Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, Vol.94, Nº886, 546

to cyber operations"[58]. *Jus in bello* rules how war is conducted but, since conflict in cyberspace is deeply *suis generis*, it is not so easy to settle a parallelism between conventional and cyber armed conflicts. Tallinn Manual declares[59] that both international and non-international armed conflicts occur whenever there are preceding hostilities, which may include cyber operations, and adds to the latter the need for a minimum level of intensity in the confrontation and organization of the parties involved. ICRC[60] views the intervention of armed forces as a clear indicator of the existence of an armed conflict, considering the longevity of the conflict or the damages irrelevant to the assessment. On the contrary, some Tallinn Manual experts[61] adopt a more restrictive point of view and rely on the duration, intensity and extension of the hostilities to determine it. "Notwithstanding this difference of opinion, it would be prudent to treat the threshold of international armed conflict as relatively low. In all likelihood, such incidents will be evaluated on a case-by-case basis in light of the attendant circumstances"[62].

The problem of attribution is crucial because the identity's authenticity is severely compromised in cyberspace, in such a way that it is relatively easy to technologically shift the blame of steering cyber operations to other people or entities located in another continent. In other words, even when cyber attacks are initiated by non-State groups, tracing results can indicate otherwise and make a third State – which was not involved by any means in the attack – wrongly accountable for the act. Complementarily, there is a thin line between countries' difficulties in catching up every single cyber attack carried out by non-State groups within its borders and passively allowing them to do it by not taking actions to refrain it from happening (for instance, focusing on investigation, criminally prosecuting cyber agents and enhancing national preventive capabilities). We must admit that it may be politically beneficial for some nations not to respect the neutrality principle[63] and become sanctuary States by acting indifferent towards cyber hostilities deriving from its territory. To conclude, there are other cases in which States

[58] *Ibid.*, 545-546

[59] Tallinn Manual, Rules 20 and 23 TM

[60] *Cf.* https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5AA133B15493D9D0C12563CD0042A15A [accessed 16 September 2016]

[61] Tallinn Manual, Rule 22 nº12

[62] *Ibid.*

[63] "Strictly speaking, the law of neutrality applies only in international armed conflict. Arguably, however, the pragmatic logic of its core principles has already found its way into practice of non-international armed conflicts as well" Melzer, N. (2011) Cyberwarfare and International Law. *UNIDIR Resources*, *Ideas for Peace and Security*, 20-21

fully comply with non-State perpetrators, by inciting, sponsoring or coordinating cyber attacks against opponents. The ICJ narrowly established effective control as the first standard for imputing responsibility to States for attacks conducted by non-State actors[64]; years later, the ICTY[65] deviated from this prior assessment and set overall control as the baseline and, following the 9/11 tragic events, there was the adoption of a new criterion based on the indirect responsibility of States[66]. The tone is now on the responsibility of States for breaches of international treaty or customary obligations against other States, by form of act or omission. That is, "(…) state responsibility for the actions of non-state actors can be said to result from a state's failure to meet its international obligation to prevent its territory from being used by such actors as a base from which to launch on other states"[67].

Furthermore, it is very important to note that, even though Tallinn Manual opines that the "[m]ere support for a group of non-State actors involved in a non-international armed conflict does not 'internationalize' the conflict (…) Some members of the International Group of Experts took the position that an international armed conflict can also exist between a State and a non-State organized armed group operating transnationally even if the group cannot be attributed to a State"[68]. The organization precondition can be observed by all means and, being cyberspace an unprecedented domain, online or virtual tools are very successful forms of organizing, acknowledging leaderships or distributing tasks which should not be disregarded. "Should such groups begin to engage in sufficiently intense operations, states are certain to begin interpreting the organizational requirements for non-international armed conflicts with greater liberality"[69]. Yet, cyber attacks executed by non-State actors, despite of its possible severity and intensity, will not be considered non-international armed conflicts.

[64] "For the United States to be legally responsible, it would have to be proved that that State had effective control of the operations in the course of which the alleged violations were committed." Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), Judgement, International Court of Justice (ICJ), 27 June 1986, §124.

[65] *Prosecutor v. Dusko Tadić (Decision on the Defence Motion For Interlocutory Appeal on Jurisdiction)*, IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1995, §120.

[66] *Cf.* http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf [accessed 10 October 2016]

[67] Graham, D. (2010) Cyber Threats and the Law of War, *Journal of National Security Law & Policy*, Vol 4:87, 96

[68] Tallinn Manual, Rule 22 nº5 and 9

[69] Schmitt, M. (2014) The Law of Cyber Warfare: Quo Vadis?. *Stanford Law & Policy Review*, Vol.25:269, 293

IV. The Impact of Cyber Power

"We sometimes forget how new cyberspace is. (…) The domain name system of internet addresses starts in 1983, and the first computer viruses were created about that time. The World Wide Web begins in 1989 (…) In 1992, there were only a million users on the internet; within fifteen years that had grown to a billion"[70]. Besides being novel and erratic, cyber power is appealing to masses because of its relatively low cost, easy access and broad reachability. When compared to conventional weapons, cyber assets produce quicker results, are easier to move around and can be almost imperceptible. As a matter of example, launching a naval offensive involves a large number of resources and personnel, thereby taking longer to plan and coordinate. The displacement of vessels along lengthy sea trajectories makes nearly impossible to disguise the conduction of the naval operation and automatically provides more time for the intended target to parry. Antagonistically, a cyber offensive operation can be carried out without previous notice by an individual equipped solely with a pocket size chip, aiming to assail a critical infrastructure of a country he or she could have never visited before.

The doctrine of war and conflict has evolved in the last couple of decades, either it terms of strategy, weapons or tactics, but one thing has remained the same: the attacker's purpose of hitting the enemy where it hurts the most. And, essentially, critical infrastructures are a nation's most valuable asset and prime concern, because an attack on one of them can compromise the remaining's regular operability. Generally speaking, "An infrastructure is considered critical when its eventual disruption has the potential of seriously affecting the social stability and the state's sovereignty. Even though different countries have distinct conceptions of CNI, all of them have in common the existence of a computerized element from which other physical elements depend"[71]. This variation of concepts is the result of the UN General Assembly's recognition of the right of each country to determine its own meaning of CNI[72]. The USA[73] characterizes CNI based on

[70] Nye, J. (2010) Cyber Power. *Harvard Kennedy School*, *Belfer Center for Science and International Affairs*, 3

[71] Natário, R. & Nunes, R. (2016) Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas [Social Risk in Cyberspace. The Vulnerabilities of Critical Infrastructures]. *Revista Militar*, Nº2547, 4; Tallinn Manual, 211

[72] U.N. General Assembly Resolution 58/199, 30 January 2004, Preamble paragraph (4)

[73] *Cf.* https://www.dhs.gov/critical-infrastructure-sectors [accessed 6 September 2016]

the importance of the sector and its susceptibility of debilitating the national security when attacked. In total, this country identifies 16 CNI, which are the sectors of chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; water and wastewater systems. On its part, the European Union has adopted a Directive on European Critical Infrastructures that focus mainly on the energy and transport sectors as well as on the assessment of the need to improve its protection. Accordingly, ECIs are defined as any "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States"[74]. The United Kingdom categorizes 13 vital sectors (communications; emergency services; energy; financial services; food; government; health; transport; water; defence; civil nuclear; space and chemicals) and determines CNI according to the "(…) major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or (…) significant impact on national security, national defence, or the functioning of the state" [75]. In Russia, the CNI term is often replaced "with the concept of 'critically important objects' (*kriticheski vazhnyh ob'ektov*, KVO) that emerged in the official policy context after 2006. The critically important objects are identified in accordance with three criteria: the type of threat, the scale of the catastrophe, and the importance of the object"[76].

The widespread high reliance on cyberspace has made our core systems and infrastructures more prone to cyber offensives, making the spectrum of CNI attacks hazardously wider. Throughout the present dissertation some examples were already uttered, however the possibilities are endless – e.g. contamination of water treatment systems, burst of water mains or sewerage, destruction of nuclear power plant turbines or oil centrifuges, tampering of confidential information, deregulation of air-traffic control, unplug of electric cell locks in a maximum security prison. But, the more worrisome is the potential cascade effect of these type of strikes – since the majority of CNI are built-

[74] Article 2 (b) of the Council Directive 2008/114/EC, 8 December
[75] *Cf.* http://www.cpni.gov.uk/about/cni/ [accessed 6 September 2016]
[76] Pynnöniemi, K. (2012) Russian critical infrastructures – Vulnerabilities and policies. The Finnish Institute of International Affairs, FIIA Report 35, 42

in vertical and horizontal models of dependency, a directed attack on one system will consequently hamper many others. For instance, in Portugal[77] the national grid is on top of the whole CNI structure, hence "(…) one prolonged malfunction on the energy supply may jeopardize the normal functioning of all CNI"[78]. It is precisely this "(…) strategic paralytic effect via the application of cyber warfare (…)"[79], also known as parallel warfare, that State and non-State cyber aggressors tend to pursue in order to evoke bulk security negative repercussions. On the contrary, "There is no national power grid in the United States. There are more than a hundred publicly and privately owned power companies that operate their own lines, with separate computer systems (…)"[80]. As a matter of fact, "Private industry owns and operates approximately 85 percent of our [USA's] critical infrastructures and key assets"[81]. This decentralized scheme can be effective in preventing the domino effect, but it certainly can compromise the harmonization of the country's national response to such serious cyber attacks (especially because private companies seldom admit they have been hacked, since such invasions forfeit their public reputation and credibility)[82].

"The greater the network integration of a target country's infrastructure, the greater its potential vulnerability"[83]. And, the 2007 attacks on Estonia are a paradigmatic example of that, not only because it was the first and most striking cyber conflict ever made public heretofore, but also because (e-)Estonia[84] was – and still is – one of the most tech-savvy and wired nations in the world. "In Estonia, 97 percent of bank transactions occur online;

[77] Where about a half of the CNI belong to the energy and transport sectors and the remaining significant part belongs to the communications and technology of information sectors. *Cf.* http://www.prociv.pt/pt-pt/RISCOSPREV/INFRAESTRUTURASCRITICAS/Paginas/default.aspx [accessed 6 September 2016]

[78] Nunes, P. (2010) Mundos virtuais, riscos reais: Fundamentos para a definição de uma estratégia da informação nacional [Virtual worlds, real risks: Foundations to the definition of a national information strategy]. *Revista Militar*, Nº2506, 4

[79] Sharma, A. (2009) Cyber Wars: A Paradigm Shift from Means to Ends. *Cryptology and Information Security Series*, Vol.3, 7

[80] Hersh, S. (2010) The Online Threat – Should we be worried about a cyber war?. *Annals of National Security*, 3

[81] Wortzel, L. (2003) Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security. Lecture 787. Retrieved from http://www.heritage.org/research/lecture/securing-americas-critical-infrastructures-a-top-priority-for-the-department-of-homeland-security [accessed 12 October 2016]

[82] "Not acknowledging attacks can leave states at risk and cedes the advantage to the attacker. Mr Borett explains that «*If organizations and individuals share their experiences, defences can be updated and adapted much more rapidly and shared much more widely to reduce the impact of these attacks.*»" *Cf.* http://www.nato.int/cps/en/natohq/news_80764.htm?selectedLocale=en [accessed 10 October 2016]

[83] Ophardt, J. (2010) Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review*, Nº3, §10

[84] "«e-Estonia» is a term commonly used to describe Estonia's emergence as one of the most advanced e-societies in the world" *Cf.* https://e-estonia.com/the-story/digital-society/business/

and in 2007, 60 percent of the country's population used the Internet on a daily basis"[85]. This strong tech-reliance made the attacks on Estonia more effective, especially since the consequences were felt in a direct way by the general society. This cyber clash began immediately after the Estonian government's decision of displacing a soviet Red Army monument to the periphery of Tallinn, on 27th of April. By coincidence (or maybe not), the day of this polemic decision coincided with the Day of Russian Parliamentarism, which motivated numerous protests of Russian nationals and sympathizers who felt offended by it. The DDoS[86] attacks lasted several weeks, at least until 18th of May, even though some small-scale cyber operations were registered afterwards; reaching the pick on the occasion of a much cherished public holiday for Russia, the Victory Day on 9th of May, entailing "[t]he only Estonian bank to report its operating losses due to the strikes estimated around $1 million in damages (…)"[87]. The overall balance of these cyber attacks was disturbing – governmental and media websites were impaired, pro-Kremlin propaganda was massively disseminated, online banking services and ATM were not operational and, during the riots boosted by President Putin, one Russian national died and more than 150 people were injured[88]. "Estonia was very near a complete digital collapse on May 10 that would have shut off many vital services and caused massive, widespread social disruptions. Luckily, Estonia's Cyber Emergency Response Team («ECERT») prevailed and Estonia avoided the worst-case scenario that many feared all too likely"[89]. All the circumstances seemingly lead Estonia to accuse Russia of sponsoring the cyber attacks, but because of the absence of proofs, inconclusiveness of the investigations and Russia's public denial of involvement, any Russian authority was brought to justice. In the aftermath of these cyber attacks only one Russian national student, living in Tallinn at the time, was convicted to pay a symbolic fine. The North Atlantic Treaty commits NATO to respond to attacks against any of its allies and "NATO has already stated in the 2014 Wales Summit that Article 5 of the North Atlantic Treaty

[85] Herzog, S. (2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, Vol.4, Nº2, 51

[86] "In sum, a Distributed Denial of Service attack (DDoS) simultaneously sends thousands of request accesses to webpages that consequently get flooded with traffic and fail to respond." Vergara, E. (2013) El derecho internacional y la seguridad cibernética [International law and cyber security]. *IEEBA Instituto de Estudios Estratégicos de Buenos Aires*, 4-5

[87] Herzog, S. (2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, Vol.4, Nº2, 51-52

[88] Radio Free Europe/Radio Liberty (2007, 9 May) Putin Warns Against 'Belittling' War Effort. Retrieved from http://www.rferl.org/a/1076356.html [accessed 18 September 2016]

[89] Shackelford, S. (2009) From Nuclear to Net War: Analogyzing Cyber Attacks in International Law. *Berkeley Journal of International Law*, Vol.27, Issue 1, Article 7, 206

can be invoked in case of a cyber attacks"[90]. But instead of activating the Article 5 and counter-attacking, NATO established a fully accredited CoE exclusively dedicated to cyber defence, in Tallinn. "CCD COE is not an operational unit, it doesn't deal with on-site attacks but, obviously it can help with its analysis. In the end, our mission is to improve the education, research and development of cyber defence"[91].

"The following year, Russian troops invaded the Republic of Georgia during a dispute over territory in South Ossetia. (…) Cyber activity against Georgian websites did not start until after Georgia made its surprise attack on the separatist movement in South Ossetia on 7 August 2008. (…) It was not until 9 August 2008 that Georgia declared a «state of war» (…)"[92]. Regardless of involving the same DDOS method, Estonian and Georgian onslaughts cannot be equated – the last one was deployed in the context of an ongoing armed conflict, which makes us induct that cyber weapons were ancillary to conventional ones, whereas the Estonian attacks were solely launched by cyber tools. Once again, important banks, governmental and news websites were hacked and pro-Russian political propaganda was scattered on them, being worthy to mention the spread of an online photo collage of Adolf Hitler and the Georgian president. Inevitably, these characteristics made Georgian authorities point their fingers at Russia, an accusation that lacked evidence base.

In 2010, the existence of a new and sophisticated worm was reported after it was detected in multiple computers around the world, with particular incidence in Iran. This malware's method was far more complex than the previous one, because it was extremely difficult to detect – the worm was developed to convey the impression that the attacked target was functioning properly and in that way mislead the users, who would be unable to notice any abnormality – and deter – Stuxnet was designed to infiltrate on specific engines or hardware with an unprecedented multiplier and auto-destruction capacity. The virus succeeded in an astonishing way: "(…) by the end of 2010, the worm had infected approximately 100,000 hosts in dozens of countries, 60 percent of which were in Iran (…)"[93] mainly in the country's clandestine and secret nuclear sites of Natanz and Bushehr. Thousands of centrifuges of both uranium enrichment facilities were damaged and there was a significant setback of the Iranian nuclear program (from twelve to

[90] *Cf.* Appendix 3 (Interview with Tomáš Minárik)

[91] *Ibid.*

[92] Brown, G. & Poellet, K. (2012) The Customary International Law of Cyberspace, *Strategic Studies Quarterly*, *US Cyber Command*, *Fort Meade*, 20755, 130-132

[93] Rid, T. (2012) Cyber War Will Not Take Place. *The Journal of Strategic Studies*, Vol.35, Nº1, 18

eighteen months[94]). Stuxnet was responsible for a mindset shift in relation to cyber power, as it exposed the vulnerabilities of the SCADA[95] system, a notion intrinsically connected with the CNI's safeguard area. In regards to the attribution of the cyber attacks, even though the USA and Israel were unofficially blamed for it, especially after some media's polemic headlines[96], no investigation confirmed the real cyber attackers.

The aforementioned three cases are the classic examples in the history of cyber conflict; but there are other significant cyber operations, although less widely spoken, that also represented a threat by exploring different ways to use cyberspace for offensive purposes. "In 1982, a trans-Siberian pipeline exploded. The explosion was recorded by US satellites and it was referred to by one US official as «the most monumental nonnuclear explosion and fire ever seen from space»"[97]. The pipeline connected Siberia to Europe and its operability required the acquisition of SCADA software, which was denied by the USA. This did not stop Russian authorities from illegally getting it and, by all appearances, it did not stop the USA from covertly inserting malware in the software and provoking the explosion. This was the first most violent cyber attack in history – "The US Air Force allegedly rated the explosion at three kilotons, equivalent to a small nuclear device"[98] – and the isolated location may have averted more disastrous consequences, particularly human casualties.

The Red October[99] virus was initially detected in 2007 and is still ongoing today, having affected more than one thousand government computers as well as multiple

[94] Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217, 222

[95] "Supervisory Control and Data Acquisition systems are network and systems of command and control conceived to support industrial processes. These systems are responsible for the monitoring and control of a large variety of processes and operations, such as gas and electricity distribution, water treatment or road transportation. (…) So, usually these systems are placed in remote locations, operate without human intervention and are only sporadically accessed by engineers or technical personnel, through telecommunications' connections incorporated into local corporate networks or even on the internet". Natário, R. & Nunes, R. (2016) Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas [Social Risk in Cyberspace. The Vulnerabilities of Critical Infrastructures]. *Revista Militar*, Nº2547, 9-10

[96] Reference to Stuxnet as being part of the "Operation Olympic Games", an alleged authorized operation by President Barack Obama – *Cf.* Sanger, D. (2012, 1 June) Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [accessed 27 September 2016]

[97] Brown, G. & Poellet, K. (2012) The Customary International Law of Cyberspace, *Strategic Studies Quarterly*, *US Cyber Command*, *Fort Meade*, 20755, 130

[98] Rid, T. (2012) Cyber War Will Not Take Place. *The Journal of Strategic Studies*, Vol.35, Nº1, 10

[99] *Cf.* Prigg, M. *(2013, 16 January)* The hunt for Red October: The astonishing hacking ring that has infiltrated over 1,000 high level government computers around the world. *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html#ixzz4NLMh4rqi [accessed 28 September 2016]

diplomatic agencies, oil and gas companies, nuclear or energy groups and research centers in around 60 countries. This unstoppable malware was designed to extract encrypted data and recover deleted files and "(…) given the current knowledge, [it is] impossible to trace down the origin of the virus, or to identify its mastermind"[100]. In our point of view, Red October's operations do not qualify to cyber attacks but to acts of espionage, because they are intended to gather classified information and are not expected to cause injury or death to persons nor damage or destruction to objects. Other interesting espionage cases in cyberspace are, for example, Titan Rain (codename for the 2003 wrongful accesses to the USA's governmental computer systems, allegedly carried out by Chinese hackers who compromised the security of the Pentagon and secret services' operations) and Moonlight Maze (this intrusion was discovered in 1999 by US Air Force who immediately convened the FBI and NSA to initiate proper investigations that concluded military maps and sensitive information have been copied by a Russian mainframe computer). Contrariwise, Shamoon[101] – a virus that affected Saudi Arabia's national oil provider by destroying computers and interrupting the company's normal operations for several days, in 2012 – "(…) seems to have been originally designed for espionage, but was then modified to destroy the files on infected computers and replace them with images of burning American flags (…) To date, Shamoon is the most damaging cyberattack ever faced by a company"[102].

More recently, in 2015, OPM publicly admitted being attacked twice by hackers who were able to steal "(…) records of current, former, and prospective Federal employees and contractors (…) sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals (…) [and] approximately 5.6 million include fingerprints"[103]. In total, it is believed that personal data of 4.2 million Federal government employees was inadvertently hacked, which represents a great risk to the country. In October of 2016, following the hacking of DNC's politicians e-mails[104], the

[100] Kessler, O. & Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26, 800

[101] *Cf.* Perlroth, N. (2012, 23 October) In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. The New York Times. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html [accessed 28 September 2016]

[102] Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217, 224

[103] *Cf.* https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [accessed 2 October 2016]

[104] Parlapiano, A. (2016, 16 August) What We Know About the Cyberattack on Democratic Politicians. *The New York Times*. Retrieved from http://www.nytimes.com/interactive/2016/08/16/us/politics/cyberattack-on-democratic-politicians-dnc.html?_r=0 [accessed 15 October 2016]

Department of Homeland Security of the USA has boldly made the first public direct accusation to Russia of trying to interfere in the up-coming national elections – "«Russia must face serious consequences. Moscow orchestrated these hacks because [Russian President Vladimir] Putin believes Soviet-style aggression is worth it. The United States must upend Putin's calculus with a strong diplomatic, political, cyber and economic response»"[105]. It is our opinion that these cyber operations do not qualify as cyber attacks, but as acts of sabotage since they are willful attempts to economically or politically defraud and weaken the targeted country.

To conclude, it is important to mention that the year of 2016 has seen a distressing growth of cyber attacks against CNI. Ukraine underwent an unprecedented power outage aroused by the BlackEnergy malware that undermined local energy providers for a couple of hours. This cyber tool "(…) has been used in attacks dating back to 2007, was originally thought to be focused on cyber espionage. But in 2014, hackers updated the toolset to include malicious code targeting SCADA ICS, known-to-be-vulnerable kit used to control power stations and other critical infrastructure"[106]. Even though the cyber attack happened in 23rd December of 2015, its consequences were only carefully examined and discussed in the beginning of the following year. In March of 2016, a USA's hospital got paralyzed for ten days as a result of a ransomware cyber attack[107] that crippled the patient records databases. Additionally, during the month of September, two Turkish hacker groups admitted having launched a cyber attack on Vienna airport that was halted by the Austrian authorities[108].

Doubting cyber power is capable of disrupting CNI has proven to be not only self-defeating, as this false sense of inviolability does not urge users to adopt a preventive stance, but also unfounded, because one cannot continue to dub this type of attack as

[105] Nakashima, E. (2016, 7 October) U.S. government officially accuses Russia of hacking campaign to interfere with elections. *The Washington Post*, Retrieved from https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html [accessed 15 October 2016]

[106] Brewster, T. (2016, 4 January) Ukraine Claims Hackers Caused Christmas Power Outage. *Forbes*. Retrieved from http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/#5ab6b3f65e6f [accessed 15 October 2016]

[107] We believe this cyber operation could be simultaneously considered a cyber crime (because it sought profit gain) and a cyber attack (because it undermined a vital infrastructure). *Cf.* Dobuzinskis, A. & Finkle, J. (2016, 19 February) California hospital makes rare admission of hack, ransom payment. *Reuters*. Retrieved from http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VS05M [accessed 15 October 2016]

[108] Austria probes alleged Turkish cyberattack on Vienna airport (2016, 7 September) Fox News Retrieved from http://www.foxnews.com/world/2016/09/07/austria-probes-alleged-turkish-cyberattack-on-vienna-airport.html [accessed 15 October 2016]

science fiction[109] when it has already happened in the past. Despite of the acknowledgement of cyber attacks like the ones mentioned above, there are authors who underestimate such possibility, with the justification given being that "(…) high priority systems are not connected to the internet, for the simple fact that its usage demand is local. This is essential to understand digital security: websites operate in completely different models than the vital systems ones, such as banking transactions systems, invoicing systems, electric control systems and even military systems"[110]. This argument couldn't be more far-fetched for the following reasons: firstly, cyberspace comprises internet but must not be reduced to it – "Telematics produce long-distance communication, via informatics, whilst cyberspace is a virtual environment that draws on these means of communication (…) So, it is understood that the Internet, despite being the world's primary telematics network, does not represent cyberspace as a whole as it is broader and may emerge from the human interaction with other technologies, like GPS, biometric sensors or vigilance cameras"[111]; secondly, "[c]yber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information – infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications"[112]; and ultimately, "(…) devices don't have to be connected to internet to be attacked. A perfect example of it is the cyber attack to the Iranian facilities, in Natanz"[113].

V. Cyber attacks and International Crimes: Crime of Aggression and War Crimes

Attribution is one of the major problems in cyberspace as it hinders the conviction of cyber perpetrators, therefore settling a sense of impunity and encouraging further cyber attacks. But, it is not the only one – the lack of reporting is a serious concern too, because only a small percentage of States publicly assume they have been victims of cyber

[109] Rid, T. (2012) Cyber War Will Not Take Place. *The Journal of Strategic Studies*, Vol.35, Nº1, 10

[110] Carreiro, M. (2012) A Guerra Cibernética: cyberwarfare e a securitização da Internet [Cyber War: cyberwarfare and the Internet securitization]. *Revista Cantareira*, Edição 17, 133

[111] Natário, R. (2013) O Carácter Trinitário da Guerra no Ciberespaço [The Trinitary Nature of War in Cyberspace]. *Revista Militar*, Nº2535, 5-6

[112] Nye, J. (2010) Cyber Power. *Harvard Kennedy School*, *Belfer Center for Science and International Affairs*, 3

[113] *Cf.* Appendix 1 (Interview with Christian Lifländer)

offensives, either due to their interest in not disclosing national security weaknesses or in using the climate of hostility as an excuse to sneakily fight back. For example, "Iran seemed reluctant even to admit its nuclear plant's computers had been affected and still does not claim to have been cyber attacked. If the damage caused by Stuxnet malware had instead been caused by a traditional kinetic attack, such as a cruise missile, it is likely Iran would have vigorously responded. (…) [I]t remains true that no state has declared another to have violated international law by a cyber use of force or an armed attack through cyberspace" [114]. First and foremost, this inertia inescapably legitimates future cyber attacks due to the absence of development of State practice and customary law. "Sometimes even *inaction* can establish practice. For example, when one state engages in conduct harmful to another, the official silence of the «victim» state can be evidence that the conduct in question does not constitute a violation of international law. This passiveness and inaction can produce a binding effect under what is called the doctrine of acquiescence"[115]. In addition, it does not propitiate an integration of this emerging threats in the existing array of international crimes and does not entail subsequent individual criminal liability. It is consensual that international law applies to cyberspace[116], however this domain's offensive operations are narrowly seen from the angle of International Humanitarian Law, being other *ad rem* branches such as International Criminal Law, usually overlooked. In point of fact, this is the main reason[117] behind the preparation of the Tallinn Manual 2.0, which is planned to be published in February of 2017. ICL sets the circumstances under which individuals are to be held criminally liable for undertaking particularly serious conducts – genocide, crimes against humanity, war crimes and crimes of aggression – suitably judged as international crimes by the ICC. "Thus the institution of international criminal courts authorized to prosecute individuals for their conduct when states do not want or are not in a position to do so is related to and directly influenced by the content of international humanitarian law

[114] Brown, G. & Poellet, K. (2012) The Customary International Law of Cyberspace, *Strategic Studies Quarterly*, *US Cyber Command*, *Fort Meade*, 20755, 132

[115] *Ibid.*, 128-129

[116] "This affirmation was reiterated in a Report on Developments in the Field of Information and Telecommunications in the Context of International Security, adopted by the United Nations Group of Governmental Experts in 2015" *Cf.* Appendix 3 (Interview with Tomáš Minárik)

[117] "The original Tallinn Manual focus on the application of International Humanitarian Law to cyberspace (mostly *jus in bello* and *jus ad bellum*), but there are many cyber attacks that don't reach the threshold of an armed attack or use of force; and those cyber attacks are also very interested in the international law application perspective. This is why the second manual will deal with this specific question in a more detailed way, because there is no doubt that international law applies to cyber attacks both in peace and war times". *Ibid.*

(…)”[118], more specifically in relation to cyber crimes committed within an armed conflict or war. In other words, the inclusion of ICL in cyberspace discourse is not meant to exclude the application of other international law norms, especially since ICL is a hybrid branch of law and “(…) simultaneously *derives its origin from* and continuously *draws upon* both *international humanitarian law* and *human rights law*, as well as *national criminal law*”[119]. Yet, an imperative question remains unanswered – what type of international crimes do cyber attacks constitute?

The crime of aggression started being discerned as an international crime during the Nuremberg Tribunal, which named it “«the supreme international crime», perceiving that aggression by one nation against another—whether motivated by politics, power, or demand for resources—formed the wellspring for the hatred form which many other heinous crimes flowed”[120]. Despite of the certainties about its untenable nature, no concrete definition of the crime of aggression was embedded in the ICC Statute, contrarily to the formal ones established for genocide, crimes against humanity and war crimes. The crime of aggression was merely posited in subparagraph (d) of the Article 5 nº1, along with a special clause that intentionally postponed the decision about its formal definition and Court’s jurisdiction in the nº2 of the same provision. Nations signed the ICC Statute on 17th July of 1998, which entered to force on 1st July of 2002; but it was only after a lengthy and complex process, that the parties decided to finally adopt the Resolution RC/Res.6, at the 2010 Review Conference in Kampala, responsible for introducing the much-anticipated legal definition of aggression. “The compromise proposals that allowed to unblock the stalemate regarding some central issues, like the Security Council role or the prerequisites for the activation of the competence on the crime of aggression, lead to the adoption of a legal regime that manifestly fell short of expectations, and in which the resolution of specific problems was held hostage by legal solutions of difficult interpretation and application”[121]. The new ICC Statute Article 8 *bis*, which proscribes the definition of the crime of aggression, in an exercise of excessive prudence which expressly defers the qualification of the international crime to the General Assembly

[118] Posse, H. (2006) The Relationship between international humanitarian law and the international criminal tribunals. *International Review of the Red Cross,* Vol.88, Nº861, 68

[119] Cassese, A. & Gaeta, P. (2013) Cassese’s International Criminal Law. *Oxford University Press*, 6

[120] Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217, 218

[121] Torres, N. (2013) O Crime de Agressão no Estatuto do Tribunal Penal Internacional [The Crime of Aggression in the International Criminal Court Statute]. *Liber Amicorum em Homenagem ao Prof. Doutor João Mota de Campo*, *Coimbra Editora*, 773-774

Resolution 3314, a non-binding document from 1974. The contemporary and hybrid forms of warfare, under which cyber conflict is included, were not contemplated in the GA Resolution, as it "(…) (1) limits aggression to the use of traditional armed force, (2) is highly State centric, (3) uses examples of traditional aggregated warfare, and (4) relies on traditional concepts of territorial integrity"[122]. To this classic and limited definition adds the fact that "(…) the ICC only has jurisdiction over crimes of aggression committed one year after thirty States Parties have ratified the amendments; and second, the States Parties must vote again, by two-thirds majority, to «enact» jurisdiction, and this vote cannot be held before January 1, 2017"[123]. Furthermore, in order to be understood as such, the crime of aggression can only be referred when both parties, victim and aggressor States, have ratified the amendments or the latter has not opted out of jurisdiction, a possibility envisaged by Article 15 *bis* nº4 and 5. Although nº2 of the Article 8 *bis* sets a list of acts that qualify as crimes of aggression, the Security Council has significant latitude in determining those, because the Prosecutor has to wait for its decision on whether the claim may proceed on the grounds of a crime of aggression or not. If no determination is made in six months, the Prosecutor may proceed with the investigation; but, if the Security Council makes a negative determination, the Prosecutor can only proceed whenever the Security Council has not invoked its power of deferral of investigation or prosecution, valid for renewable periods of 12 months, under Article 16.

Even though the crime of aggression has to target and be perpetrated by a State, hence excluding non-State organizations or members from the scope of the ICC's jurisdiction, the Security Council has already once acknowledged a non-State actor as an aggressor. This extraordinary position was reflected in the Resolution 405, on 14th April of 1977, regarding to the aggressions against Benin carried out by an invading force of mercenaries[124] and is now duly included in the nº2 (g) of the Article 8 *bis*. "In addition, few commentators regarded acts of aggression as acts that can be carried out by states or «similar entities». However, these sources cannot by themselves indicate any change or

[122] Ophardt, J. (2010) Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review*, Nº3, §30

[123] Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217, 220

[124] "The Security Council (…) *Strongly condemns* the act of armed aggression perpetrated against the People's Republic of Benin on 16 January 1977" *Cf.* Resolution 405 (1977), 14th of April

a nascent perception of the ability of non state actors to carry out acts of aggression and, thus, the ability of their members to be liable for the crime of aggression"[125].

Regrettably, it sounds obvious that these characteristics seriously constraint any prospect ICC conviction of cyber attacks as crimes of aggression but still do not preclude that possibility. This international crime pursues the protection of the international peace throughout the condemnation of persons who hold a leadership position in any State's hierarchy of public offices. Hypothetically speaking, and ignoring the obstacles that attribution represents in cyberspace, even if we could prove a political or military State leader executed a cyber attack against other country, it would be necessary to subsume that action to the Article 8 *bis* nº2 list of acts of aggression. Based on a literal analysis of the disposition – parties used the expression '*Any* of the following acts' instead of '*Only* the following acts' – it is our opinion that the list is not exhaustive; plus, "(…) the norm expressly remits to the Resolution 3314 («in accordance with»), from which it *verbatim* took that list. And the catalogue of Article 3 of the Resolution 3314 is not closed, since the Security Council can qualify other situations as acts of aggression, besides those contemplated ones (Article 4 of the Resolution 3314, which *expressis verbis* refers that the enumeration is not exhaustive)"[126]. Consequently, certain analogies can be explored for illustrative purposes: the act of invasion (Article 8 bis nº2 (a)) is akin to an installation of a computer virus or malware that allows the aggressor to occupy the target's space and have unlimited access to the stored information and data; an annexation (Article 8 bis nº2 (a)) is similar to a botnet[127] attack, because it provides the attacker direct control over the 'zombie' computer; a blockade (Article 8 bis nº2 (c)) is comparable to a DDoS attack, due to the fact that it makes the target become unavailable and paralyzed; if a nation permits other State to launch attacks from its own territory (Article 8 bis nº2 (f)) it becomes a sanctuary State and it seems logic that this conduct will be prohibited regardless of the conventional or cyber nature of the attack[128]. For these reasons, and since

[125] Cohen, A. (2013) Prosecuting terrorists at the International Criminal Court: Reevaluating an used legal tool to combat terrorism. *Michigan State International Law Review*, Vol. 20:2, 249-250

[126] Torres, N. (2013) O Crime de Agressão no Estatuto do Tribunal Penal Internacional [The Crime of Aggression in the International Criminal Court Statute]. *Liber Amicorum em Homenagem ao Prof. Doutor João Mota de Campo*, *Coimbra Editora*, 784

[127] English abbreviation for robots' network; "*Botnets* provide remote control of the infected PC to the perpetrators. Those are a nightmare for system's administrators and one of the most profitable businesses for cyber criminals, who rent these networks' time for the DDoS, for the transmission of computer viruses and for the distribution of *spam",* Vergara, E. (2013) El derecho internacional y la seguridad cibernética [International law and cyber security]. *IEEBA Instituto de Estudios Estratégicos de Buenos Aires*, 4-5

[128] Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217, 234

the ICC has the authority to unreservedly interpret the notion of aggression[129], we do not believe there is any plausible reason to exclude cyber attacks that reach the threshold of wrongful uses of force and armed attacks from the interpretation of the acts of aggression. In order to do that, it is necessary to broadly read the provisions and to establish an analogical nexus between cyber and conventional acts of aggression.

The idea of cyber war has been insistently rebutted by allegations that "Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future"[130]. We oppose these arguments on the grounds that past events are not an infallible indicator of today or tomorrow's reality. Although we agree that "Not one single past cyber offense, neither a minor nor a major one, constitutes an act of war on its own"[131], we do not see the merits to delve the concept of war as a stand-alone act. "Historically, the initiation of a war depended upon a formal act of State, generally a «declaration of war». (…) This traditional understanding of war has fallen into desuetude (…)"[132] and so has the strategic thinking, given to the emergence of cyber power. Nowadays, it is not advantageous to deploy only one type of weapon during a war. Instead, nations resort to different kinds of tools and equipment whenever they partake in war because their ultimate goal is to defeat the adversary, so the more resources they have, the more chances there are to prevail. Despite of the number and nature of the weapons employed by each party during the conflict, as long as the offensive operations have a political purpose and a violent or destructive aim and means they should be considered acts of war.

War crimes result from grave breaches of customary and conventional IHL rules (Article 8 nº2 (a) of the ICC Statute) and from unlawful acts executed during an international (Article 8 nº2 (b)) or non-international (Article 8 nº2 (c) (e)) armed conflict, whenever there is a casual link between the two; and, contrarily to the crime of aggression, any person can be prosecuted for committing war crimes. Although Article 8 provides a list of war crimes that does not have any reference to cyberspace, the existing rules should not be interpret in a limiting or prejudicial way (Article 10). "The regulation of war crimes in the ICC Statute, while meritorious in so many respects, can be faulted in other respects;

[129] ICC Statute, Article 15 *bis* nº9

[130] Rid, T. (2012) Cyber War Will Not Take Place. *The Journal of Strategic Studies*, Vol.35, Nº1, 6

[131] *Ibid.*

[132] Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, *The National Academies Press*, 152

indeed, it would seem that such regulation marks a retrograde step with regard to existing international law"[133]. We have previously enunciated some cases that attest cyber power's capability of destructing and appropriating property or intentionally targeting civilian population, objects and even facilities like hospitals, for instance. Curiously or not, all of these examples are envisioned by the war crimes list of the ICC Statute (respectively, Article 8 nº2 (a) (iv); (b) (i), (ii), (ix)).

Most of cyber attacks are not carried out in this type of context – in fact, "[t]erms like 'cyber attacks' or 'cyber terrorism' may evoke methods of warfare, but the operations they refer to are not necessarily conducted in an armed conflict"[134]. But for those that are, and recalling there was an ongoing armed conflict between Georgia and Russia in 2008, it is not understandable why there is still so much reluctance in admitting such attacks as acts of cyber war. Perhaps, this assumption is inhibited by the inexistence of direct human injuries or deaths. "The point of absence of casualties is still the ultimate benchmark when declaring the existence of a war. Without loss of human life, people find it difficult to believe in cyber war, even though you lose money or electricity, for example"[135]. However, the possibility of cyber attacks directly or indirectly causing human damages or losses is not so ludicrous, especially when considering the unpredictable effects of a cyber attack against CNI. In our perspective it will, sooner or later, eventually happen and we are not the only ones who believe in this scenario[136].

Conclusion

"For the time being, cyberwarfare has not had dramatic humanitarian consequences, and it is to be hoped that this state of affairs will not change in the future. The potential for human tragedy, however, is already enormous, and it is likely to increase with our growing dependence on computer-controlled systems to sustain our daily lives"[137]. This being said, this dissertation's spirit should not be associated with views that refuse the

[133] Cassese, A. & Gaeta, P. (2013) Cassese's International Criminal Law. *Oxford University Press*, 80

[134] Droege, C. (2012) Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, Vol.94, Nº886, 542

[135] *Cf.* Appendix 1 (Interview with Christian Lifländer)

[136] With a similar perspective: "I only see the situation deteriorating and getting much worse, so at one point there could also be losses of human lives" *Cf.* Appendix 1 (Interview with Christian Lifländer); "I am sure that human injuries or deaths as a result of cyber attacks are possible and probably will happen in the future" *Cf.* Appendix 3 (Interview with Tomás Minárik).

[137] Melzer, N. (2011) Cyberwarfare and International Law. *UNIDIR Resources*, *Ideas for Peace and Security*, 36

possibility of cyber attacks being perceived as crimes of aggression or war crimes. Despite recognizing the limitations of the extension of Article 8 *bis* definitions by analogy, we do not consider such interpretative exercise prohibited by Article 22 nº2 of the Roma Statute, because the list of crimes is not exhaustive and does not constituted by traditional 'elements' of the crime[138]. Relatively to war crimes, for us there are no doubts that the only thing that changes from conventional war to cyber war is the platform or means from which the attacks are launched. All forms of warfare end up complementing and reinforcing each other, being this multiplier role an added value to the parties in conflict and we do not see valid reasons for cyber to be any different.

It is clear cyberspace challenges all the classic legal concepts – from the notions of use of force and armed attack to the characterization of international crimes – and this dissertation's purpose was to reflect on the advent of this mindset shift precipitated by the affirmation of cyberspace as the fifth domain. Nations have to be prepared to respond to global cyber threats and we believe the way forward is to enhance international cooperation – "(…) as for example agreeing on sharing information of national organizations and mechanisms to tackle cyberspace misuse, sharing national taxonomies (…)"[139]. Other authors lean towards the implementation of a cyber treaty that, in order to be effective, would need to "(…) overcome obstacles in several areas: enforcement, security, privacy, free speech, corporate liabilities and responsibilities, and foreign policy"[140]. We believe the majority of States are not interested in restricting operations in cyberspace or controlling the manufacturing of cyber tools and that cyberspace does not lack regulation. Cyber operations are not settled on a legal vacuum and the number of legal frameworks and concerted efforts is growing – for instance, the Directive on security of network and information systems adopted by the European Parliament on 6th of July 2016; the creation of an Informal Cyber Working Group by OSCE that adopted a second set of Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies in March 2016; the 2010 U.N. Report of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security; the Yekaterinburg Declaration issued by the Shanghai Cooperation Organization on 16th of June 2009.

[138] Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217, 234

[139] *Cf.* Appendix 2 (Interview with Rogério Raposo)

[140] Denning, D. (2001) Obstacles and Option for Cyber Arms Controls. *Georgetown University*, 2

Subsequently, instead of reinforcing offensive cyber capabilities with the institution of cyber armies[141], countries should adopt a cooperative and prophylactic attitude in cyberspace.

[141] China Confirms Existence of Elite Cyber-Warfare Outfit the 'Blue Army' (2011, 26 May) *The Fox News*. Retrieved from http://www.foxnews.com/tech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit.html [accessed 15 October 2016]

Appendix nº1

The following questions were presented to **Mr. Christian-Marc Lifländer**, **Deputy Head for Policy at the Cyber Defence Section of the Emerging Security Challenges at the NATO Headquarters**, in the form of a phone interview conducted on 28th of October 2016 by Ms. Rafaela Miranda:

1. **What is NATO's core task in the areas of cyber security and cyber defence?**

NATO's primary purpose is to guarantee the protection of its own networks. It is unequivocal that NATO, unlike any other existing international organizations, has a unique kind of mandate. When comparing NATO to EU or European Commission, for example, we realize that none of them have such a mandate like we do – we are a political and military alliance. Despite of the current landscape of multiple and fast technological advances, our defensive mandate remains the same, not only for cyberspace but also for other domains. NATO also acts as a platform in advancing the capability's developments amongst allies by identifying the capability needs of the alliance, determining how best to respond to them and providing mechanisms to fulfill all the requirements.

2. **What are the main goals set by NATO for the next decade?**

Even though technology is changing very quickly, which makes it difficult to answer this question with detail, our mandate is the Washington Treaty and keeping the territory and population of the alliance safe. Currently, the focus is on the implementation of the cyber defence policy. On that note, we want to establish and develop partnerships with academia, partner countries (for example Japan, South Korea and Mediterranean countries) and international organizations (especially with the EU). The EU is discussing the cyber phenomenon in a broader view, when compared to the military and strategic perspective NATO undertakes. For example, EU deals with national infrastructures and NATO doesn't, but leaves that responsibility to the allies. In fact, the two organizations have different mandates. So it's NATO's interest to promote complementarity and coordination with the EU, rather than to duplicate efforts. We also want to take cyber defence business to a next level by increasing national resilience with the goal of having the Alliance be better protected. To sum up, NATO's core tasks and mandate for the next decade are likely not going to change, but the way we implement this mandate could very well change. Not only because of the different kinds of technology that need to be put in place, but also due to the partnerships NATO has to establish, that have to include the industry as well. An example that demonstrates our interest in a win-win situation, not only multi-nationally, but also with small enterprises, could be the Individual Cooperation Programme. Innovation is key, especially because the industry sector is responsible for the products we all use. This is being aware that cyberspace involves several actors and techniques, so if the industry shares their insights with us, we could all benefit from it.

3. Do you consider that the general society is fully aware of the potential impact and consequences a cyber attack might originate?

Not really! And the reason is very obvious: we interact with technology in different ways, some of us are constantly updating their smartphones and others are late bloomers, but both tend to forget the cyber security aspect of technology. The same happened when cars were invented – initially, there was no need for inspections, driving lessons nor driver's license, but today's reality is completely different. In cyberspace, we're still living in a 'wild west', there is unevenness in users' awareness for the need of taking precautions. Only sporadically, people tend to react to incidents (the *Yahoo* case is an example of it). If there is the need for a change of e-mails or credentials, people usually not even feel it, because security is taken for granted… Until something really serious happens. It's like washing our hands – it is a mundane thing, but the more we do it, the less chances you have of getting ill. So, if we pay more attention to our behavior in cyberspace, we will likely avoid really bad results. I would say that lack of user's awareness and simple or unintentional (and potentially malevolent) behaviors of not efficiently responding to phishing attacks, software or firewalls problems are the biggest reasons behind the magnitude of cyber attacks. The user is one of the weakest links of the equation.

4. What do you think could be done to revert this paradigm?

I think it has to go beyond the simple awareness campaigns. It would be easier to start at a young age, perhaps already in kindergarten and from primary school until university, by introducing people to better uses of technology, its benefits and dangers, teaching them how to protect themselves and how to stay safe in cyberspace. I firmly believe that what you learn at an early age will stay with you for the rest of your life. This type of education should be universal and be directed to children and grownups, public and private organizations and companies. Apart from awareness programs, we would be well advised to educate workforce in organizations and companies – in order for employees to be allowed to use computers at the workplace, they should periodically pass a test and those who fail should lose access to it. Any strategy to improve habits will have to take into focus the human being and there are different ways to do it. Recently, I had the opportunity to interact with the industry sector and I realized the awareness of people in senior positions is very meager. Many don't use computers and they either don't understand the technology or are afraid of it.

5. Several authors refer to information and cyber assets as unlimited powers, which can either be used against us or in our favour. Is it NATO's aim to control the use of cyber power or simply to mitigate its effects?

Like I said before, NATO is but one actor in cyberspace. There are also governments, companies, NGOs, media, private citizens… NATO Secretary General has declared that NATO has a very specific role in cyberspace. It is not NATO's aim to militarize the internet. Vice versa. Also, there are laws that we recognize that apply in this space (IHL and LOAC), especially when it comes to the use of force. It's important that this message comes across very clearly, because isn't our intention to somehow control the cyberspace.

6. Cyber attacks are still considered to activate the Article 4 of the North Atlantic Treaty, which calls upon members to "consult together", but does not bind them to "assist each other", as would be required under Article 5. Politically speaking, should it be any different? Why or why not?

This is an interesting question... I can say it is inter changeable. Assistance can also be the sharing of malware signatures or technical knowledge, but it can also be diplomatic, economic and military cooperation. As you know, NATO has only invoked Article 5 once before – after the 9/11 terrorist attacks – and since the attribution wasn't clear at the time, the response wasn't bound by time, or by means. Similarly, when thinking about the meaning of both Articles, I believe there are a lot of different ways to look at Article 5: it could be considered a political decision, a judgement to de-escalate the situation and so on. But members could consult and assist each as well under Article

4, there isn't a precondition. The way we interpret Articles 4 and 5 always comes down to the meaning of assistance and consultation. Cyberspace is an interesting field in comparison to the conventional world. There has to be an armed attack for the activation of Article 4 and when it comes to cyber attacks they occur almost on a daily basis, but you don't invoke Articles because of that. Cyber attacks happen constantly and allies assist each other in conformity, either on incident management, handling or exchanging data and info, in order to become more aware and improve how they deal with this. We have different platforms to deal with cyber attacks rather than invoking those two Articles.

7. **Should countries that are more developed and advanced in terms of cyber capabilities and weapons help the ones that are lacking behind, either in terms of offensive and defensive mechanisms?**

I will express my personal opinion, because NATO has not expressed an official position on this. All countries, big or small, are facing the same situation... So, the smart thing to do is to deal with resilience. Working on cyber offensive tools needs to come secondary for your need to be able to defend yourself first. Also, one needs to pay close attention to what countries want to achieve with it and whether they have a clear objective in mind. Offensive tools can be expensive and they cannot be a substitute for defensive capabilities, that's why I'm not so sure everybody should develop them to the fullest extent. When you think about the details of it, if you want to manufacture and develop cyber weapons, you might actually end up losing money should your cyber weapon not work, because the target has changed operating system. In the end, this capability is expensive. The average time to find vulnerabilities is several months, so this is what you should be taking into account. That's why I believe it is important to focus on the defensive side.

8. **The occurrence of a dominant cyber attack on a national military infrastructure or armed forces would wreak havoc, especially considering this type of target as unassailable. Should it be created in all military services a special unit dedicated to cyberspace? If so, what would be the biggest challenges?**

NATO recognizes cyberspace as a domain which means we will have to deal with protection, defence, threats and execution of missions as we do in any other domains. Instead of focusing on information protection, we now want to focus on mission assurance. In practical terms, instead of dealing with vulnerabilities at a technical level we will deal with it at an operational level. Indeed, NATO advises allies to set up relevant structures to deal with the cyber phenomenon. The biggest challenge, however, is going to be on the change in mindset. Like I said previously, our mandate stays the same but we will address it from a different angle, because we have to change our business model. NATO's biggest challenge for the future isn't really cyber, but more related to policy. Cyber is best dealt in a more whole of government manner, not only delegating it to the Ministry of Defence, Foreign Affairs or Interior, for example, in order to increase the level of response.

9. On the 26th of September, during the first presidential debate of the United States of America, there was a segment called "Securing America" and its first question was about cyber warfare. Curiously, both candidates answered based on external threats and national enemies, rather than on preventive capabilities. Is there any reason to expect and fear a 'Digital Pearl Harbor' any time soon?

Intellectually speaking it's an interesting question, but when considering past incidents (Estonia, Stuxnet, Sony, OPM or DNC, for example) we realize none of them amounted to a 'Digital Pearl Harbor'. In the coming years, there will be many more devices and the number of attacks is likely to increase. If nothing is done to develop further our resilience, it is not impossible that one day something will happen. For now, it's only a theoretical concept. In fact, in order to reach the same impact as Pearl Harbour, the cyber consequences would likely have to be complemented with conventional ones. I went to the list of past attacks and the worst and most common ones were cyber exploitation, espionage and sabotage. Yet, none of them led to full destruction. In relation to the US debate, I also watched it and similarly found it interesting that none of the candidates mentioned the NIST framework or made new suggestions on how to improve national resilience.

10. There are some authors who address cyber warfare in a very sceptical way. Right away, I can recall Marcelo Carreiro (who doubts about the possibilities of undermining CNI not connected to internet) and Thomas Rid (who identifies cyber war as mere sabotage, subversion or espionage). What is your opinion about it?

Regarding the first author, I haven't read anything from it, but I can certainly say that the devices don't have to be connected to internet to be attacked. A perfect example of it is the cyber attack to the Iranian facilities, in Natanz. As for Thomas Rid, I can say I'm familiar with his opinion and I think he correctly points out the fact that none of the attacks, until today, had the same level of physical destruction that one could compare to a conventional war. But my counter argument to him is that you have to take a look at concept of war and ask about its meaning… The point of absence of casualties is still the ultimate benchmark when declaring the existence of a war. Without loss of human life, people find it difficult to believe in cyber war, even though you lose money or electricity, for example. While this interpretation might have been correct in the past, we don't know what will happen in the future nor to what extent will our societies be dependent on services potentially affected by cyber attacks. I tend to agree with Thomas Rid, but on the other hand I'm sure we could eventually witness human casualties and losses in the future. Being a cyber criminal is already a profession. There are people doing this for a living and outsourcing their services to state actors. I only see the situation deteriorating and getting much worse, so at one point there could also be losses of human lives.

11. Which cyber perpetrators are more dangerous – states or NSG?

In terms of quantity, NSG are more dangerous because they are very numerous (hackers, hacktivists, criminal organizations, terrorists, etc). But at the same time their activities are limited due to the lack of funding, resources or also by very specific focus or agenda they may have in mind (crime, money, etc). States have better capabilities and more resources to invest in it, but still you might have a group or an individual that's very potent and capable in outsourcing its services to a nation. So, the money might come from a nation but the delivery of negative effects is up to a single person. There is no exact answer to this question, we are better served by focusing on the activity, rather than its origin.

12. What do you envision as the future of cyber international norms?

I think we are all waiting on the Tallinn Manual 2.0, but until then we will continue using *jus in bello*, there is no need to create international treaties but to use the existing ones and make sure they correctly apply to cyberspace. Also, it's up to states' behavior in cyberspace to see whether the existing body of international law will suffice or not. There are some bilateral agreements (China with both United Kingdom and USA, regarding economic espionage) but I believe it's prudent to wait and see what will happen in the next years.

It is relevant to mention that **Mr. Christian-Marc Lifländer fully cooperated and authorized Ms. Rafaela Miranda to include all the answers in her Master Dissertation on Cyber Warfare**, by accurately quoting him as the interviewee.

Appendix nº2

The following questions were presented to **Mr. Rogério Raposo**, **Head of Policy and Strategic Development Department of the National Cybersecurity Center of Portugal**, in the form of an online interview conducted on 5th of October 2016 by Ms. Rafaela Miranda:

1. **The Portuguese National Cyber Security Center started its mission in 2014, seven years later than the first and more notable cyber attack occurred in Estonia. What took so long for the creation of such an important center?**

The Portuguese National Cybersecurity Centre (PT NCSC) started, indeed, its mission in October 2014. The process to create such a structure, at national level, being complex and dependent on operational and legal decisions/provisions, is normally preceded of preparatory and exploratory assessments, in order to ensure that the right structure is created in the right (or necessary) time, with the necessary powers and authority. The first reference to the creation of the PT NCSC occurred in a Council of Minister's Resolution of 2012, following a legal reference for the need of a National Information Security Strategy, in 2011. Upon the referred Resolution in 2012, a multi-stakeholder Commission was created to set up the terms, structure and mission of the National Cybersecurity Centre. Still in 2012 the referred Commission concluded and delivered a report with the necessary actions and foundations (including the governance of Cybersecurity issues) to create The Portuguese National Cybersecurity Centre, which (due to several political and economic constraints) was formalized in May 2014.The underlined question, regarding the gap between 2007 and 2014 and the possible national vulnerability in terms of tackling cybersecurity issues has, however, to be addressed in terms of competences and mechanisms. I believe it's necessary to state that cybersecurity, at national level, was not left unattended due to the inexistence of the PT NCSC. Since before 2007 Portugal had a fully operational national CSIRT and several other private and industry CSIRTs, having the national CSIRT liaison responsibilities in the most significant and important CSIRT networks worldwide.

2. **Do you think the Portuguese civil society has fully awareness of the consequences and magnitude of a cyber attack launch? Also, and in comparison with**

the average preparation of other countries, is Portugal ready to face and fight back a potential cyber attack?

Awareness is a continuous process in all societies worldwide, and one of the main concerns in all nations. The awareness level in Portugal is as it is in most of the European countries, with a high level of awareness in technical communities and a not so high level among the rest of the society. The threat that a cyberattack poses to each and everyone's privacy and rights is understood and known (even feared by some), but the necessary human behaviour in preventing such attacks is a challenge for everyone, including governments (who are concerned with questions of sovereignty, fundamental rights and economic development), industry (concerned with intellectual property and reputation of their products) and academia (seeking constantly for the development and discussion of the future solutions and competences).

The response to a national cyberattack is not (cannot be) an individual response, being Portugal a member of the European Union and NATO. Portugal has the necessary competences, as other Member and Participant States, to respond in coordination with its partners (nations and industry).

3. In order to guarantee the stability and equality of all the member states in terms of cyber defence, do you believe European Union should have a network of cyber security centers and policies, all of them with the same techniques and resources, operating closely in this matter?

That will be, I believe, a consequence of the constantly evolving dependence on cyberspace and of some legal measures taken recently in the European Union, as is the Network and Information Security Directive. As stated in the previous question, the protection and reaction to threats in cyberspace is a collective endeavour and European Union, including its Member States, are aware of that fact. More than similar techniques and tools, the focus shall be put upon competences and knowledge sharing, seeking not only redundancy at this level but essentially complementarity and well defined procedures and processes to achieve a coherent and coordinated response.

4. International cooperation is key for preventing cyber threats from escalating to more serious and harmful events. What are the main steps and precautionary measures that need to be adopted in this context?

In line with what has been written above, the PT NCSC has been participating and collaborating both at national and international level, ensuring and affirming its responsibility as the Portuguese National Cybersecurity Authority and PoC (point of contact) for these issues (being the most relevant the EU, OSCE and NATO – along with the Portuguese National Cyberdefense Centre). All steps and measures must be prepared and taken at operational and strategic level, and for this Portugal has the necessary instruments and measures in place. The main steps and precautionary measures to be adopted (again, not only at national level but with nations that are willing to cooperate in the security of cyberspace) are interdependent and bilaterally complementary both at operational and strategic level. Steps that are based on building confidence and trust, as for example agreeing on sharing information of national organizations and mechanisms to tackle cyberspace misuse, sharing national taxonomies and agreeing on not to willingly conduct or allow cyber activities against critical information assets, have a strong consequence in opening cooperation and communication channels to prevent more serious and harmful events. Nations need to build and consolidate bonds in these domains, through cooperation, transparency and stability.

5. The Decree-Law 69/2014, 9th of May was responsible for implementing the Portuguese National Cyber Security as well as establishing its aims, one of which is to work on the early warning of cyber attacks that have public interests and national critical infrastructures as prime targets. What type of measures are being studied and applied by the Portuguese National Cyber Security Center? And, what are expected to be the most negative and severe effects that a cyber attack on the aforementioned targets could implicate in Portuguese territory?

Early warning is, in fact, one of the attributions of the PT NCSC and, pursuing its achievement, work is being done to establish the necessary technical tools and institutional/inter-organizational processes that will allow a single, reliable and contextual situational awareness of cyberspace under Portuguese "responsibility". Visibility over cyberspace is essential for predictive measures and to understand trends that are likely to affect Portuguese interests through (and in) cyberspace. The most severe and negative impacts in Portugal (as in any other nation) need to be divided in terms of its physical, societal and economic impacts, hence there isn't really a direct and sustainable answer to the question regarding "the most …". Any severe disruption on Critical Infrastructures is plausible to produce large economic and societal effects, with possible physical repercussions. A large and severe attack to the financial system will produce a cascade effect on every nation's growing digital market, with repercussions on several links of every supply chain and every market. A large and severe attack or disruption on public services, which are essential for the normal functioning of every service provided by a nation to its citizens, will most likely result in social tensions and (if originated from another nation) diplomatic tensions as well. A holistic answer would necessarily be "any attack or action that causes a disruption on essential services, vital for the well-being and normal functioning of a nation".

6. What situation nationally and internationally do you envision for the next decades in the cyber domain, essentially in terms of prevention capacity, national defence programmes and growth of hostility capabilities?

Reflecting a personal opinion and vision, cyberspace needs to be addressed as one more layer in the existing stack of tools, instruments and technologies that are available for national and societal development. Its particularities are in fact unique and different from anything else that has been made available until now (its resilience, global implementation and outstanding availability to everyone/everywhere), going beyond traditional borders and out of reach of what has been the traditional State's control.

Nations already acknowledged the need for global, regional and sub-regional agreements on these issues, recognising that it is impossible for a single nation to protect itself, to protect others or to respond effectively to the challenges posed by a crescent impulse of organized and sophisticated cybercrime. Prevention will need to be articulated, at minimum, on a sub-regional level and national defence programmes will necessarily (as today) be set in light of what are the actual defence programmes and alliances, consistent with the geopolitical context at the time.

It is relevant to mention that **Mr. Rogério Raposo fully cooperated and authorized Ms. Rafaela Miranda to include all the answers in her Master Dissertation on Cyber Warfare**, by accurately quoting him as the interviewee.

Appendix nº3

The following questions were presented to **Mr. Tomáš Minárik, Law & Policy Researcher at NATO Cooperative Cyber Defence Centre of Excellence (National Security Authority of the Czech Republic),** in the form of an in-person interview conducted on 14th of October 2016 by **Ms. Rafaela Miranda** at the CCD COE, in Tallinn, Estonia.

1. The NATO Cooperative Cyber Defence Centre of Excellence, located in Tallinn, is an International Military Organization and the only NATO-accredited CoE exclusively dedicated to cyberspace related matters. What is CCD COE's mission and mandate? And, what has it achieved since it was created in 2008?

The Centre is a think tank – this is be the better word to describe it. CCD COE supports NATO in its tasks and transformation efforts, but it is not part of NATO's structure. That is why NATO has 28 member countries and we have 16 sponsoring nations (Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States), plus 2 contributing participants (Austria and Finland). CCD COE is based on voluntary contributions, so all NATO nations that want to take part of our cooperation projects can become members at any time. There are more states applying and I am sure CCD COE's members will grow in number in the coming years.

CCD COE is not an operational unit, it doesn't deal with on-site attacks but, obviously it can help with its analysis. In the end, our mission is to improve the education, research and development of cyber defence. In order to do that, we focus on 4 main tasks: realization of technical, legal and operational trainings and courses; publication of books and articles; organization of international conferences; and, enhancement of capability, cooperation and information sharing through consultation, workshops and exercises. Over the years, CCD COE has accomplished some successful achievements. For example, the Tallinn Manual is our most recognized book and we are currently working on the Tallinn Manual 2.0, which will be published in February of 2017. Every year, around 500 decision-makers and experts participate in our biggest conference, called CyCon. We also have the Locked Shields international exercise, which is a very practical and advanced annual real-time network defence exercise.

2. The Tallinn Manual is considered by many the cyber-bible. Why do we need a second version? What will be the major differences between the two manuals?

It will not be a change, but an optimization, an addition or supplement. The original Tallinn Manual focus on the application of International Humanitarian Law to cyberspace (mostly *jus in bello* and *jus ad bellum*), but there are many cyber attacks that don't reach the threshold of an armed attack or use of force; and those cyber attacks are also very interested in the international law application perspective. This is why the second manual will deal with this specific question in a more detailed way, because there is no doubt that international law applies to cyber attacks both in peace and war times.

3. Do you think we should not look into cyberspace only in the optics of IHL but also in other branches.

Yes, definitely. All International Law applies to cyberspace and this is the universal consensus now. This affirmation was reiterated in a Report on Developments in the Field of Information and Telecommunications in the Context of International Security, adopted by the United Nations Group of Governmental Experts in 2015. Even states like China or Russia agree on it, despite of their strong opposition to the idea of militarization of cyberspace.

4. There are several and sometimes contradictory definitions of cyber attacks, not only provided by authors, but also by CCD COE official website's cyber dictionary. In your opinion, what is a cyber attack and how can we distinguish it from other cyber operations (e.g. sabotage or espionage)?

There are many definitions of cyber attacks, but I believe definitions are only useful in the context we use it. The same term can mean different things in different contexts, for example the concept of 'necessity' is not the same in International Humanitarian Law or in domestic laws. The same happens with the term of cyber attack. According to the Tallinn Manual, cyber attack is defined for the purposes of *jus in bello* (Rule 30) and you can only apply it when there is an ongoing conflict. But, of course, outside an armed conflict cyber attacks can also take place and, in those situations, you need a different definition. So, it changes depending on the context, regime and circumstances.

In the end, I would say that the distinction between what NATO and the national systems consider as CNA or CNE is kind of artificial, because in both cases you are trying to get into computer systems without authorization. The technique is the same and only the purpose is different. But, how are victims supposed to know what is the attacker's purpose? I am leaning towards treating all these activities in the same manner. You can call it cyber attacks, but legally you can only consider it as cyber attack when a penal code or an international agreements expressly says it.

5. Many authors express doubts regarding the occurrence of a cyber war in the future, on the ground that there was no cyber conflict capable of directly causing human injuries or deaths until now. When does a cyber operation surpass the level of an attack and becomes an initiation of a war in cyberspace?

I am sure that human injuries or deaths as a result of cyber attacks are possible and probably will happen in the future, even though is everyone's wish to prevent it from happening. Any cyber attack should be judged by its effects, so if a cyber attack directly or indirectly causes human injuries or deaths, I don't see why it should be treated any differently from kinetic attacks. Also, it's very difficult to separate cyber from the other areas, once you have kinetic effects, the situation will probably escalate very quickly. I hope cyber war never happens, but states will definitely use cyber means in order to gain advantage over other countries. For example, Thomas Rid declared that cyber war will never take place and I think I'm forced to agree with him on this… Why would states do that? Launching a cyber attack on other countries' CNI will most likely negatively affect the attacking country as well. And, of course, all of this depends of what you define as war: if you consider it as an armed conflict, I am sure cyber means will not be the only ones involved. That is why I believe cyber is inseparable from other domains.

5.1 In that perspective, can we consider the Georgian 2008 attacks as cyber war?

I think it is reasonable to put that case in those terms… Since the cyber attacks were launched in the context of an armed attack, I would consider it cyber war.

6. Cyber attacks are still considered to activate the Article 4 of the North Atlantic Treaty, which calls upon members to "consult together", but does not bind them to "assist each other", as would be required under Article 5. Do you think it is

fair that victimized countries are not provided with the assistance from other nations, especially the ones that are more technologically advanced?

States have multiple ways of dealing with cyber attacks – military, law enforcement or counter intelligence responses – but, all of them along with the cyberspace developments indicate that we are going in the direction of improving cooperation and having common or collective responses, as it happens in any other domain. And, actually, I have to disagree with you on the invocation of the Articles. NATO has already said in the 2014 Wales Summit that Article 5 of the North Atlantic Treaty can be invoked in case of a cyber attacks. Even though it doesn't set the criteria for the activation of the Article, NATO is very clear on this.

6.1 Yet, facing the Estonian cyber attacks, neither Article 4 nor 5 was invoked…

Of course, the invocation of the Articles depends also on the countries, the response to cyber attacks also depends on them. I would say that we should reserve this type of response to more serious cyber attacks. The Tallinn Manual takes a reasonable stand on this and even with bullets flying across the borders, there are no certainties about what will activate the Article 5 of the Treaty.

7. Do you believe there is the need of a Cyber Treaty?

States are not interested in a Treaty for obvious political reasons, so I don't see any possibility of that happening in the future. But, it could be interesting to see law in place and it certainly would make our lives easier, because we would have universal definitions and rules applicable to cyberspace.

8. Sanctuary states are problematic for cyberspace, because assessing lack of commitment or deliberate omissions is extremely difficult. How can we make sanctuary states more accountable for cyber states that are launched from their territories?

In these cases, it should be applied the laws of state responsibility. There is always the principle of due diligence, countries are responsible for what happen inside their boarders and for their cyber infrastructure inside their country. And if they choose to tolerate the launch of cyber attacks from their own country, despite on the warnings of other states, then they should face the consequences and assume responsibility for it.

9. Cyber attacks happen, we discuss their impact but, in the end, there are never international sanctions or convictions applied to cyber perpetrators, neither there is many interest from the victimized countries to revert this paradigm. Do you think this will change in the future?

It probably will, in relation to cyber attacks that provoke devastating consequences, for example human injuries and deaths. States always do things according to their interests… And for example, with Iran, I think it's pretty obvious why there was no official complain. Also, victimized states don't really have an interest in escalating the conflict, that is why sometimes they choose to remain silent.

10. What are the main aims set by CCD COE's for the next decade?

We want to continue to give advice to the states, in order for them to take more active roles in cyberspace. Additionally, we want to keep on providing training to scholars and policy-makers I don't expect any abrupt developments, I think we will see some kind of improvement in terms of public accountability of intelligence services in some states. On the other hand we will see improvement of cyber capabilities, both offensive and defensive.

It is relevant to mention that **Mr. Tomáš Minárik fully cooperated and authorized Ms. Rafaela Miranda to include all the answers in her Master Dissertation on Cyber Warfare**, by accurately quoting him as the interviewee.

Bibliography and List of References

Articles and Monographs

Brown, G. & Poellet, K. (2012) The Customary International Law of Cyberspace, *Strategic Studies Quarterly*, *US Cyber Command*, *Fort Meade*, 20755

Carreiro, M. (2012) A Guerra Cibernética: cyberwarfare e a securitização da Internet [Cyber War: cyberwarfare and the Internet securitization]. *Revista Cantareira*, Edição 17

Cassese, A. & Gaeta, P. (2013) Cassese's International Criminal Law. *Oxford University Press*

Chayes, A. (2015) Rethinking Warfare: The Ambiguity of Cyber Attacks. *Harvard National Security Journal*, Vol.6

Cohen, A. (2013) Prosecuting terrorists at the International Criminal Court: Reevaluating an used legal tool to combat terrorism. *Michigan State International Law Review*, Vol. 20:2

Colarik, A. & Janczewski, L. (2012) Establishing Cyber Warfare Doctrine. *Journal of Strategic Security*, Volume 5, Nº1, Article 7

Denning, D. (2001) Obstacles and Option for Cyber Arms Controls. *Georgetown University*

Droege, C. (2012) Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, Vol.94, Nº886

Graham, D. (2010) Cyber Threats and the Law of War, *Journal of National Security Law & Policy*, Vol 4:87

Hathaway, O. & Crootof, R. (2012) The Law of Cyber-Attack. *Yale Law School Legal Scholarship Repository*, *Faculty Scholarship Series*, Paper 3852

Hersh, S. (2010) The Online Threat – Should we be worried about a cyber war?. *Annals of National Security*

Herzog, S. (2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, Vol.4, Nº2

Hollis, D. (2007) Why States need an International Law for Information Operations. *Lewis & Clark Law Review*, Vol.11:4

Kessler, O. & Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26

Melzer, N. (2011) Cyberwarfare and International Law. *UNIDIR Resources*, *Ideas for Peace and Security*

Miller, K. (2014) The Kampala Compromise and Cyberattacks: Can there be an international crime of cyber-aggression?. *Southern California Interdisciplinary Law Journal*, Vol.23:217

Natário, R. (2013) O Carácter Trinitário da Guerra no Ciberespaço [The Trinitary Nature of War in Cyberspace]. *Revista Militar*, Nº2535

Natário, R. (2016) O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço [Combat against Cybercrime: Anarchy and Order in Cyberspace]. Revista Militar, Nº2541

Natário, R. & Nunes, R. (2016) Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas [Social Risk in Cyberspace. The Vulnerabilities of Critical Infrastructures]. Revista Militar, Nº2547

Nunes, P. (2004) Ciberterrorismo: Aspectos de Segurança [Cyberterrorism: Security Aspects]. Revista Militar, Nº 2433, 1

Nunes, P. (2010) Mundos virtuais, riscos reais: Fundamentos para a definição de uma estratégia da informação nacional [Virtual worlds, real risks: Foundations to the definition of a national information strategy]. Revista Militar, Nº2506

Nye, J. (2010) Cyber Power. Harvard Kennedy School, Belfer Center for Science and International Affairs

Ophardt, J. (2010) Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. Duke Law & Technology Review, Nº3

Posse, H. (2006) The Relationship between international humanitarian law and the international criminal tribunals. International Review of the Red Cross, Vol.88, Nº861

Pynnöniemi, K. (2012) Russian critical infrastructures – Vulnerabilities and policies. The Finnish Institute of International Affairs, FIIA Report 35

Rid, T. (2012) Cyber War Will Not Take Place. The Journal of Strategic Studies, Vol.35, Nº1

Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press

Schmitt, M. (2010) Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts. Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press

Schmitt, M. (2012) International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Harvard International Law Journal, Volume 54

Schmitt, M. (gen. ed.) (2013) Tallinn Manual on the International Law Applicable to Cyberspace, Cambridge University Press

Schmitt, M. (2014) The Law of Cyber Warfare: Quo Vadis?. Stanford Law & Policy Review, Vol.25:269

Shackelford, S. (2009) From Nuclear to Net War: Analogyzing Cyber Attacks in International Law. Berkeley Journal of International Law, Vol.27, Issue 1, Article 7

Schreier, F. (2015) On Cyberwarfare. DCAF Horizon, Working Paper Nº7

Torres, N. (2013) O Crime de Agressão no Estatuto do Tribunal Penal Internacional [The Crime of Aggression in the International Criminal Court Statute]. Liber Amicorum em Homenagem ao Prof. Doutor João Mota de Campo, Coimbra Editora

Vergara, E. (2013) El derecho internacional y la seguridad cibernética [International law and cyber security]. IEEBA Instituto de Estudios Estratégicos de Buenos Aires

Online Articles or Reports

Dutch Advisory Council on International Affairs and Advisory Committee on Issues Of Public International Law (2011) Cyber Warfare Report, Nº77 AIV/Nº22

CAVV, 21. Retrieved from http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf [accessed 10 September 2016]

Wortzel, L. (2003) Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security. Lecture 787. Retrieved from http://www.heritage.org/research/lecture/securing-americas-critical-infrastructures-a-top-priority-for-the-department-of-homeland-security [accessed 12 October 2016]

Online Newspaper Articles

Adm. Michael Rogers on the Prospect of a Digital Pearl Harbor. (2015, October 26) *The Washington Post*. Retrieved from http://www.wsj.com/articles/adm-michael-rogers-on-the-prospect-of-a-digital-pearl-harbor-1445911336 [accessed 17 September 2016]

Austria probes alleged Turkish cyberattack on Vienna airport (2016, 7 September) *Fox News*. Retrieved from http://www.foxnews.com/world/2016/09/07/austria-probes-alleged-turkish-cyberattack-on-vienna-airport.html [accessed 15 October 2016]

Brewster, T. (2016, 4 January) Ukraine Claims Hackers Caused Christmas Power Outage. *Forbes*. Retrieved from http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/#5ab6b3f65e6f [accessed 15 October 2016]

Brownlee, L. (2015, July 16) Why 'Cyberwar' Is So Hard To Define. *Forbes*. Retrieved from http://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/1/#664ba43c2eaa [accessed 2 September 2016]

China Confirms Existence of Elite Cyber-Warfare Outfit the 'Blue Army' (2011, 26 May) *The Fox News*. Retrieved from http://www.foxnews.com/tech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit.html [accessed 15 October 2016]

Dobuzinskis, A. & Finkle, J. (2016, 19 February) California hospital makes rare admission of hack, ransom payment. *Reuters*. Retrieved from http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VS05M [accessed 15 October 2016]

Nakashima, E. (2016, 7 October) U.S. government officially accuses Russia of hacking campaign to interfere with elections. *The Washington Post*, Retrieved from https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html [accessed 15 October 2016]

Parlapiano, A. (2016, 16 August) What We Know About the Cyberattack on Democratic Politicians. *The New York Times*. Retrieved from http://www.nytimes.com/interactive/2016/08/16/us/politics/cyberattack-on-democratic-politicians-dnc.html?_r=0 [accessed 15 October 2016]

Perlroth, N. (2012, 23 October) In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. The New York Times. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html [accessed 28 September 2016]

Prigg, M. (2013, 16 January) The hunt for Red October: The astonishing hacking ring that has infiltrated over 1,000 high level government computers around the world. The Daily Mail. Retrieved from http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html#ixzz4NLMh4rqi [accessed 28 September 2016]

RadioFreeEurope RadioLiberty (2007, 9 May) Putin Warns Against 'Belittling' War Effort. Retrieved from http://www.rferl.org/a/1076356.html [accessed 18 September 2016]

Sanger, D. (2012, 1 June) Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [accessed 27 September 2016]

Websites

www.ccdcoe.org/tallinn-manual.html [accessed 2 September 2016]

https://www.dhs.gov/critical-infrastructure-sectors[accessed 6 September 2016] https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5AA133B15493D9D0C12563CD0042A15A [accessed 16 September 2016]

http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf [accessed 10 October 2016]

http://www.nato.int/cps/en/natohq/news_80764.htm?selectedLocale=en [accessed 10 October 2016]

https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [accessed 2 October 2016]

http://www.prociv.pt/pt-pt/RISCOSPREV/INFRAESTRUTURASCRITICAS/Paginas/default.aspx [accessed 6 September 2016]

http://www.state.gov/s/l/releases/remarks/197924.htm [accessed 4 September 2016

Legal Instruments and Rulings

Additional Protocol I and II

Council Directive 2008/114/EC, 8 December

Geneva Conventions

ICC Statute

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, International Court of Justice (ICJ), 27 June 1986

Oil Platforms (Islamic Republic of Iran v. United States of America), Summary of the Judgement, International Court of Justice (ICJ), 6 November 2003.

Prosecutor v. Dusko Tadić (Decision on the Defence Motion For Interlocutory Appeal on Jurisdiction), IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995

U.N. Security Council Resolution 405 (1977), 14th of April

U.N. General Assembly Resolution 58/199, 30 January 2004