DOI:10.21544/1809-3191/regn.v22n2p261-290

STATE-SPONSORED CYBER-OFFENCES

Marcelo A. O. Malagutti[1]

ABSTRACT

In the post-industrial societies, computers are ubiquitous and pervasive. Besides, they are interconnected. As these characteristics give unprecedented productivity, they also present risks never faced before. Cyber offences pose the threat of powerful nations, both in the military and economic dimensions, being confronted by much weaker states, or even proto-states or terrorist groups. At the same time, *cyber superpowers* have the ability of remotely and surreptitiously coerce opponents without deploying troops in the field. This paper outlines the threats posed by state-sponsored cyber-offences and analyzes their characteristics, describing their applications in the light of some traditional military concepts, and also their motivations, the nature of their operations, the *warriors* and the *weapons* used.

Keywords: Cyber. Offences. Power Projection. Area Denial. Software Power.

[1] Master in Arts in War Studies candidate at the Department of War Studies of King's College London, London, United Kingdom. E-mail: marcelomalagutti@yahoo.com.br.

INTRODUCTION

Cyber-offences' perpetrators, generically called *hackers*, have been divided into four different groups: cybercriminals (sometimes subdivided into individuals and organized as distinct groups), hacktivists, terrorists, and nation-states. Each of these groups has different motivations, scope of actions, targets, and resources, and thus deterrence and dissuasion options (MALAGUTTI, 2016b). Although clearly possible to concede that any of these groups could be state-sponsored, and used in an escalation strategy to destabilize an opponent state, this work will focus on the direct threats posed by nation-states to their peers, considering their motivations, the nature of their operations, the *warriors* and the *weapons* used so far.

THE MOTIVATIONS

Nation-states have many motives to promote cyber-offences. The Snowden case revealed some. The first one has been political espionage, related to the personal communications of the Brazilian and Mexican Presidents, the German Chancellor, and some of their Ministers, amongst thousands of others. Outside the political realm, Snowden also revealed the espionage of Petrobras, the Brazilian state-owned oil company, that a couple of years before had announced the discovery of massive oil reserves in Brazilian waters (GREENWALD, 2014). A third real motivation connects to security and defence through surveillance, with bulk collection of metadata regarding phone calls, e-mails, messaging, file transfer and many more communication methods (GREENWALD, 2014; HIMR..., 2011; OPERATIONAL..., 2016). All of the above examples relate to *intelligence gathering*.

Besides the motives presented, related to "peacetime", there are also the traditional wartime military motivations of *projection of power* and *area denial* on the cyber domain. Cyber-offences perpetrated with existing technologies are unlikely to cause massive casualties directly (RID, 2012; RID; MCBURNEY, 2012). However, they could still serve as "effective means of political coercion or brute force" (LIFF, 2012). Influence and coercion of an opponent nation-state, by means of sabotage, if not an act of war, have been the aims of Stuxnet (DAVIS, 2015; FALLIERE; O'MURCHU; CHIEN, 2011; LANGNER, 2011; SANGER, 2012; ZETTER, 2011).

And then there is... financial profit! Until very recently this motivation had always been related to cybercriminals, and never to states. However, a series of attacks against the SWIFT network has been linked to North Korea (PERLROTH; CORKERY, 2016).

In the following pages, each of the above motivations is explored in larger detail.

INTELLIGENCE GATHERING

For our purposes, we consider *intelligence gathering* as divided into two areas: *surveillance*, as the passive collection and analysis of information, and *espionage* as the active one.

Surveillance

Communications Intelligence (often referred as COMINT) has always played a major role in security and defence matters. The Roman emperor Julius Caesar (100 BC to 44 BC) already used a transposition cypher algorithm, to avoid his enemies' understanding of captured messages (SINGH, 2000, p. 14-20).

A particular function of COMINT is *signals intelligence* (SIGINT). The Government Communications Headquarter (GCHQ), the agency responsible for SIGINT in the United Kingdom (UK), defines it as "intelligence derived from intercepted signals" (HIMR..., 2011, p. 9). It has become more and more relevant since the advent of the telegraph. GCHQ's website remarks the importance of the interception of the famous Zimmerman Telegram as one of the main reasons for the United States having entered WWI (OUR..., [201-?]). Radio communications made SIGINT even more important, and GCHQ's website also points the history of Bletchley Park, where Alan Turing and his team created Colossus, the first computer in history, that helped to decipher the German Enigma code, a valuable asset for winning WWII. The entire operational structure of Bletchley Park was based on "passive SIGINT", with the interception and transcription of every message sent by the Germans (bulk interception or collection), for subsequent analysis and deciphering. Thus, a surveillance operation.

History also shows that DARPA has sponsored the creation of the foundations of Internet. Moreover, the process of passive SIGINT based on the Internet nowadays is quite similar to that of WWII (HIMR..., 2011, p. 9-12).

In recent years, "the Internet is a major source of comparable intelligence power today" (OMAND, 2015). For the NSA it has become even easier, since

> As the Internet developed, a large portion of the Internet backbone passed through the United States, meaning that many foreign-foreign communications could be accessed by surveillance done inside the US. Previously, foreign-foreign communications would have been accessed outside of the US, where the US Constitution and various laws are less strict than for access inside the US (SWIRE, 2015).

Espionage

In the *cyber* context, however, intelligence gathering is not a passive task only. The UK Government has recently presented to the Parliament a case for keeping its bulk powers granted by Investigatory Powers Act 2000, not only for Bulk Interception but also for Bulk Interference (EQUIPMENT..., 2016). In its Code of Practice for Equipment Interference there is a list of activities allowed when there is "risk for the UK security" (OPERATIONAL, 2016, p. 7):

a) obtain information from the equipment in pursuit of intelligence requirements;

b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;

c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);

d) enable and facilitate surveillance activity by means of the equipment.

It is important to observe that these activities do not need to be targeted to a particular computer, device, or even user. They can be conducted on sets of equipment, for instance in an entire building or village, anywhere in the world, if there is the suspicion of a "risk for the UK security" in that *area*.

Its counterpart, the U.S. NSA, has been granted the legal (by the American law) right to spy on 193 countries. The exception is their Five Eyes partners (Australia, Canada, New Zealand and the UK), considered "out of limits" by the Foreign Intelligence Surveillance Court under the Foreign Intelligence Surveillance Act of 1978 (KEDMEY, 2014).

Similarly, the U.S. Supreme Court has recently granted the

Federal Bureau of Investigations (FBI) the possibility of hacking computers worldwide, based only on warrants given by American judges. Until then, a judge in a U.S. state could only give orders limited to that state (KHANDELWAL, 2016; YADRON, 2016). One of FBI's missions is counter-intelligence. Thus, to defend the U.S. against espionage, FBI is legally authorized to hack computers outside the U.S.

What information is aimed by cyber espionage? It can be political, military or economic information from or about another government; or theft of trade secrets or intellectual property from private corporations or universities (CILLUFO; CARDASH; SALMOIRAGHI, 2012). Cyber theft of military technology from universities is not new, with a famous case having being reported already in 1989 by Clifford Stoll in his seminal The Cuckoo's Egg (STOLL, 1990). Indeed, in the early stages of the Internet.

The clear intent of economic espionage is "to increase the economic prosperity or viability of business concerns in a given state", and although state-directed, its "ultimate beneficiaries may be private or semi-private entities" (CILLUFO; CARDASH; SALMOIRAGHI, 2012).

The U.S. government frequently accuses China of "stealing" technical, military and economic information. American authors argue in the same direction, saying that "foreign intelligence services" engage in industrial espionage in support of private companies and that "an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress" is stolen every year "from networks maintained by U.S. businesses, universities, and government agencies" or that as national power is intimately connected with economic vitality, sustained intellectual property losses allegedly could erode U.S. power (LYNN, 2010).

Other recent cases show that the U.S. is not the only victim of this activity. The Norwegian intelligence service publicly accused the Chinese of stealing sensitive data and state military secrets from Norway-based firms (MURDOCK, 2016). The Swiss government has accused the Russians of being connected to the cyber espionage of the state-owned military supplier company RUAG (GOVCERT.CH, 2016). The Germans have accused the Russians of being behind attacks to the Bundestag (WAGSTYL, 2016a).

However, a European Parliament report released in 1999, and the facts revealed in the Snowden case in 2013, showed that the NSA is also engaged in economic espionage gaining "enormous advantage for American industry" (CAMPBELL, 1999; GREENWALD, 2014, p. 138).

Ultimate aims of espionage "include the desire to influence decisions, and affect the balance of power (regionally, internationally, and so on)" (CILLUFO; CARDASH; SALMOIRAGHI, 2012).

Indeed, during the recent U.S. presidential elections, the U.S. intelligence community has attributed to Russia the hacking of the e-mail accounts of members of the Democrat Party and the leaking of selected information in a way of favouring the Republican candidate, declaring the Russians intended to influence the results of the American presidential elections (PALETTA, 2016). The next day, President Obama stated the White House was studying 'proportional' responses, while the day after Mr. Sergei Lavrov, Russia's Foreign Affairs Minister, said to CNN 'we do not deny', but 'we have not seen a single fact', a 'single proof'. 'If they decide to do something, let them do it', said Mr. Lavrov (KREVER; SMITH-SPARK, 2016). The Republican candidate eventually won, although having more than one million votes less than the Democrat candidate. Just a week after the U.S. elections, the Chief of German Intelligence announced that Germany is worried about possible Russian influence in the German elections, to happen in 2017 (WAGSTYL, 2016b; GERMAN..., 2016).

MILITARY AFFAIRS

In 1993, just after the end of the Cold War, Arquilla and Rondfeld declared "Cyber War Is Coming" (ARQUILLA; RONFELDT, 1993). Since then the debate about what would (or would not) constitute cyberwar, cyber weapons, cyber warfare, or cyber domain gained more and more space in the popular imagination, in the media, in policy making and the academia.

In this hype, there are considerations regarding the direct or indirect effects of a cyber attack in terms of lethality or physical harm to people, machinery or buildings, that could characterize the use of violence (CLARKE; KNAKE, 2010; MAHNKEN, 2011; RID, 2012; STONE, 2013). There are discussions regarding cyber as the fifth warfighting domain, after land, sea, air and space (ESTADOS UNIDOS, 2013; LIBICKI, 2012). The debate involves strategic and conceptual considerations, questioning if cyber would not be part of information or electronic warfare, or if it would not be considered just a force multiplier traversing all other domains ((KOPP, 2010; STONE, 2007; MAHNKEN, 2011; SHARMA, 2010; ESTADOS UNIDOS, 2013). There were also some more metaphysical considerations, as the fact of cyber being human-made while the four previous where God's

creation, fortunately already grounded (DENNING, 2015; LIBICKI, 2009).

These discussions aside, the fact is the pervasiveness of information systems in modern armed forces has simultaneously "empowered and imperiled" military forces (ARQUILLA, 2011). To understand how, it is useful to analyse the role of cyber in some of the basic military functions.

Projection of Power and Area Denial

In political science and military jargon *projection of power* consists in the ability to apply national power out of national boundaries. Military traditional examples include aircraft carriers and ballistic missiles. More recently *drones* have become a popular example.

It is reasonable to conceive that a CNA might be used by a state to project force without physically placing conventional military forces in the field, with lower costs and no risk of casualties (LIFF, 2012).

Area denial relates to denying the adversary the ability to bring into (or freely using within) the contested region its operational capabilities (RUSSELL, 2015). Traditional examples can be minefields, caltrops or the *dragon teeth* used on the famous Siegfried Line.

How to implement area denial in cyber? An immediate answer seems to be shutting down the Internet! As mentioned above, the creation of the Internet has been sponsored by DARPA. During the cold war, the U.S. military was worried about the risks of a nuclear first-strike from USSR to destroy the U.S. possibility of retaliation. Hence, the solution has been a development designed for resiliency.

> While much of the physical infrastructure of cyberspace is relatively unprotected, located on beaches, along railways, and in buildings in densely populated areas, very little of that critical infrastructure is critical by itself. The nodes and cables may be relatively exposed and potentially vulnerable, none is singularly important to the entire system. The infrastructure consists of redundant cables and satellites for private sector communications and military operations. The logic programming of the data and telecommunications was designed to adapt to changing circumstance, to automatically route traffic through an alternate route when the first route is unavailable. This "self-healing" property of cyberspace makes it difficult to cause substantial damage without launching a full assault against the infrastructure (RUSSELL, 2015).

Thus, an attack aiming the destruction of the physical infrastructure of the cyberspace in a well-connected country is virtually impossible.

Besides, cyber power can be divided into two categories: *Software Power* and *Hardware Power* (MALAGUTTI, 2016b). As explained above, destroying the hardware could be ineffective for projecting power. Nevertheless, considering the *Software Power* perspective, it is not necessary to destroy hardware to achieve power projection or area denial.

A good example of *Software Power* capabilities is provided by Eligible Receiver, an exercise promoted by the U.S. Joint Chiefs of Staff in June of 1997 to test U.S. computer defences. The proposed scenario was that of a crisis that forced Washington to send troops and aircraft to South Korea quickly. Thirty-five specialists of the National Security Agency (NSA) composed the *red team*, simulating hackers in service of North Korea to subvert the American operation, using only publicly available equipment and information. In just two weeks, using only commercial computers and hacking programs downloaded from the Internet, they have been able to "simultaneously break into the power grids of nine American cities and crack their 911 emergency systems". Established "civilian chaos and distracted Washington", the *hackers* attacked the Pentagon's computer networks and got access to 36 of them, becoming able to "roam freely across the networks, sowing destruction and distrust wherever they went", for instance directing supplies to wrong destinations, possibly incapacitating last generation jet fighters due to the lack of fuel, replacement parts, or ammo (ADAMS, 2001).

Since the *hackers* have promoted their attacks remotely, without physical (or proximity) access to the targets, they have projected power. Moreover, since they have limited the operational capabilities of U.S. military forces, they have imposed area denial. Without physical destruction, since the networks were still there. However, they could not be trusted by the U.S. military.

Disruption and Force Multiplier

There are two major concepts regarding the uses of military cyber capabilities. The first one relates to strategic cyber warfare, as the capacity of accomplishing huge effects in complete surprise. The second one relates to operational cyber warfare, used in support of conventional military in battle (ARQUILLA, 2011).

Operational cyber war has the potential to amplify physical operations, and it is relatively inexpensive, it is worth developing, although not only a question of technique but also requires the understanding of how potential opponents use information to wage war (LIBICKI, 2009, p. xx). As an example of operational cyber capabilities, allegedly the Chinese have an ingenious tactic for inserting computer viruses through the air into three models of reconnaissance and surveillance planes used by the U.S. Air Force. They wage the attack via electromagnetic waves targeting the onboard surveillance systems that emit a signal, what could disrupt the airplane's controls and cause its crash (HARRIS, 2014, p. 63).

Indeed, cyber attacks are unlikely to be decisive, and the damage (or disruption) caused by a successful cyber attack will probably be more ephemeral than a kinetic one since defenders may be able to recover the affected systems in short time. The greatest benefit of cyber warfare will probably come from its use in conjunction with, or as an enabler of, conventional kinetic military means, as Israel did in Operation Orchard in 2007 (LIFF, 2012; MAHNKEN, 2011; RID; MCBURNEY, 2012).

Command-and-Control (C2) for many non-cyber military capabilities is so heavily reliant on cyberspace that an opponent could be tempted to seek a crippling first-strike it (MORGAN, 2010). Perhaps the most significant effect of Eligible Receiver has been the fact that the *hackers* have also been able of paralyzing the human C2 system with high level of mistrust originated by fake orders from a commanding general, "bogus news reports on the crisis and instructions from the civilian command authorities".

> As a result, nobody in the chain of command, from the president on down, could believe anything. This group of hackers using publicly available resources was able to prevent the United States from waging war effectively (ADAMS, 2001).

This process is usually referred as *decapitation*, intended to disrupt the internal cohesion of the adversary and that could potentially cripple the attacked state's defending military forces and increase the effectiveness of a subsequent kinetic attack (LIFF, 2012).

One way of avoiding decapitation of retaliatory cyber capabilities is decentralizing them, and both the Chinese and the American military, traditionally command-centric, seem to be working in the development of decentralized cyber capabilities. China is developing military cyber

capabilities in some of its militia units that compose the second level of reserves of their military forces, typically assigned to local civil defence tasks (AUSTIN, 2016b). The U.S. also plan to employ its second level of reserves, the National Guard, in cyber activities (AUSTIN, 2016b; SHALAL, 2016).

Cyber clearly offers a new set of resources to be used by military strategists for achieving political ends, either as force multipliers, incapacitating the enemy in preparation for kinetic strikes, or as strategic coercive tools to be used instead of kinetic strikes. Americans, Russians, and Chinese, among others, have published their defence strategies including cyber operations as part of their military capabilities and missions.

Coercion

The anonymity provided by cyberspace also enables a flexible coercion strategy, allowing the compelling measure to be conducted privately and the victim to respond actions with "less concern about the influence of third parties or the demands of conclusive attribution" (HARE, 2012).

Coercion has been the purpose of Stuxnet, by means of sabotage, if not an act of war (FALLIERE; O'MURCHU; CHIEN, 2011; LANGNER, 2011; SANGER, 2012; ZETTER, 2011). For the first (known) time a software tool has been used by a nation-state to impose its political will onto another, using violence, as the physical destruction of machinery, and even direct lethality, as being used against a nation's vital interest. Thus, in "Clausewitzian" terms, an act of war. Cyberwar. Stuxnet "succeeded in disrupting and delaying Iranian nuclear efforts, by some accounts to an extent rivalling the effects of a limited military strike" (KISSINGER, 2014, p. 345). Stuxnet might have been the U.S. option to avoid an Israeli air strike against the Iranian facilities at Natanz, similar to that of Operation Orchard, when Israeli jets bombed an alleged nuclear Syrian facility in the Deir ez-Zor area (SANGER; MAZZETTI, 2016).

Recently uncovered information shows that Stuxnet was the spearhead of a much larger operation named Nitro Zeus, "devised to disable Iran's air defenses, communications systems and crucial parts of its power grid" (Ibid). Since Iran signed a nuclear control agreement, Nitro Zeus "has been shelved, at least for the foreseeable future" (Ibid). Had the compelling intent of Stuxnet not worked, a broader range of cyber attacks would have been triggered, in an escalation still in the cyber domain. This exemplifies a gradual shift

from tactical force multiplier to strategic warfare (SHARMA, 2010).

Not only the Americans have used cyber power for sabotage. In December of 2016 a power shortage in Ukraine has been caused by a series of cyber attacks attributed to Russia, that however not complex in structure have been well coordinated, leaving more than 80,000 people without energy (ZETTER, 2015).

Financial Profit

Until very recently financial profit had always been considered an objective of cyber criminals, and not of states. A series of attacks on the SWIFT network, a Brussels-based banking consortium that runs what is considered the world's most secure payment messaging system, however, has been attributed to North Korea by the security firm Symantec. The attacks have been conducted thru banks in the Philippines, Vietnam, and Bangladesh. Even experienced security researchers declared never previously having seen attacks carried by a nation-state for stealing money (PERLROTH; CORKERY, 2016).

THE OPERATIONS

The examples given characterize cyber operations. They are generically named Computer Network Operations (CNO) and can be divided into three subsets: Computer Network Exploitation (CNE), Computer Network Attack (CNA) and Computer Network Defence (CND) (EUROPEAN PARLIAMENT, 2011, p. 7). These types of CNO and its characteristics are detailed below. Intelligence gathering and spying CNO are often called CNE. A different kind of CNO is named CNA and aims to "destroy or otherwise incapacitate enemy networks" or the confidentiality, integrity and availability (the CIA triad) of information in the targeted networks (SCHNEIER, 2014). It is important to observe that the major difference between CNE and CNA regards their objective, since "technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyber warfare can well be cyber espionage initially – or simply be disguised as such." (EUROPEAN PARLIAMENT, 2011, p. 7) Both CNE and CNA are offensive operations and consist, basically, of hacking opponent's computer networks (SCHNEIER, 2014). The last group of CNO, and the only defensive one, is named CND and

aims to defend computer networks from both CNE and CNA. Amongst the most frequently cited characteristics of CNOs are:

- Its asymmetry in comparison with conventional or nuclear weapons.
- The attribution difficulty and "plausible deniability".
- The offensive advantage resulting from the difficulty of effective CND.
- The difficulty of deterring cyber attacks.

THE WARRIORS

Freedman (2015, p. 228) posed the following question: "Might an army of software wizards use insidious electronic means to dislocate the support systems of modern societies, such as transport, banking and public health?". Besides the importance of software power in this question, an interesting aspect of it is: who integrates this "army of software wizards"?

Profile

As offensive operations are essentially hacking activities, the "software wizards" that perpetrate them are hackers.

The profile of a hacker fits that of the "ideology of violation" which "holds that things which it is possible to steal deserve to be stolen, and the security of things that are guarded ought to be tested to destruction by those with sufficient technical nous to do so" (BETZ; STEVENS, 2011, p. 34). They are classified according to the kind of hacking they practice. *White hats (or ethical hackers)* are non-malicious ones that "explore networks for their own enjoyment or testing its security on behalf of its owners", who make their living "discovering holes in systems and then alerting the manufacturer or developer so that they can be patched". *Black hats (or crackers)* are malicious hackers that "break into a system for some other purpose" (BETZ; STEVENS, 2011, p. 25; HARRIS, 2014, p. 67).

> Progressively, hacking has become more objectively purposeful. [...] Criminals co-opted hackers for criminal purposes; governments co-opted them for purposes of state, including espionage and war; and hackers as human individuals have voluntarily attached themselves to all sorts of social movements and causes out of whim or conviction (BETZ; STEVENS, 2011, p. 33).

Hackers may "be off the government payroll but linked to a particular political faction or individual politicians (more likely in non-Western states)". They may also be superpatriots with no formal connection with their government but "striking at adversaries in lieu of or in advance of where they are sure the government would go" or acting as proxies of their governments (LIBICKI, 2009, p. 46). However, cyber warriors are hackers in state employ, perhaps in uniform, acting "in the cause of specific policy objectives", that can "be employed to create and operate malware, such as the Stuxnet worm" (BETZ; STEVENS, 2011, p. 26).

While private hackers are more likely "to use techniques that have been circulating throughout the hacker community", "state hackers can tap a larger and more secretive research effort that can consolidate discoveries, tools, and techniques across their own organization". They are also likely to be "disciplined in attacking certain targets for certain reasons and avoiding others that may look equally interesting but are not part of the plan" (LIBICKI, 2009, p. 47).

Recruitment and Training

The recruitment of cyber warriors by U.S. armed forces and the NSA is very comprehensive. Each armed force branch has developed a set of aptitude tests "to determine whether someone might be suited to network maintenance and defence or shows promise for the rarer, more sophisticated offensive missions". They have also inserted basic training in cyber security for all officers, while all "five military service academies now include cyber warfare as a field of study". The best hackers of each one participate in a competition sponsored by the NSA, whose specialists act as a *red team* to test their skills. The final step in the "education of cyber warriors is on-the-job training" (HARRIS, 2014, p. 61).

The military have also "urged colleges and universities to teach cyber warfare", and the NSA has worked together with some universities to help writing their curriculum. In some cases, candidate students have to pass a background check and get a security clearance, since "part of the coursework includes classified seminars at the NSA", which in some cases even provide scholarships and monthly stipends for students of computer science that after graduation have to work for NSA. The undergraduate courses develop the basic and defence skills. The agency then complements the training for offensive operations (HARRIS, 2014, p. 66).

The recruitment happens even at undergraduate levels. A program

named CyberPatriot, a nationwide competition for middle and high school students, sponsored by the military and cosponsored by defence contractors, helps to identify young talents in the field. "NSA also recruits from the best computer science schools, including Stanford University and Carnegie Mellon. Additionally, it sends representatives to the most important annual hacker conventions, Black Hat and DefCon Las Vegas." (HARRIS, 2014, p. 67)

The British GCHQ, by its side, works on the accreditation of Master (MSc) courses, having already 18 courses of 14 universities certified (OUR..., 2016).

THE WEAPONS

The literature is plenty of different names for cyber threats: virus, worms, botnets, Trojans, malware, rogue code, logic bombs, and so on. However, all of them have two things in common: they consist of software (software power!), and they have to be somehow implanted in the targeted networks. An *implant* is a piece of software designed to activate or enable a subsequent action; in many cases, they allow the attacker to send (or load) attack code that the target system will run causing damage to its functions or integrity (LIBICKI, 2010). In this section we detail the main features of cyber-weapons.

The Anatomy of Software Weapons (or the Cyber Kill Chain)

A typical modern Advanced Persistent Threat (APT) is a multi-phase attack software tool, for either CNA or CNE operations, usually based on the Intrusion Kill Chain (HUTCHINS; CLOPPERT; AMIN, 2010). Each phase relates to different functions performed at different times by the software for offensive actions. The seven original phases of the Intrusion Kill Chain have been rearranged in the thirteen steps of the Industrial Control Systems (ICS) Cyber Kill Chain, presented below (ASSANTE; LEE, 2015):

- *Reconnaissance*: consists in the examination, possibly with the support of human intelligence (HUMINT), of the target to find possible "weaknesses and identify information that supports attackers in their efforts to target, deliver and exploit elements of a system".
- *Weaponization*: "includes modifying an otherwise harmless file", such as

a PDF or MS Word document, "for the purpose of enabling the adversary's next step".
- *Targeting*: "is the process of analyzing and prioritizing targets and matching appropriate lethal and nonlethal actions to those targets to create specific desired effects".
- *Delivery*: consists in the attacker finding a "method to interact with the defender's network", for instance, a phishing e-mail used to deliver a weaponized PDF.
- *Exploit*: "is the means the adversary uses to perform malicious actions", for instance when the weaponized PDF is opened.
- *Install*: is the consequence of the well-succeeded exploitation, for instance when the opened weaponized PDF installs an implant or malware or connects a VPN.
- *Command and Control (C2)*: consists in establishing a connection to the previously installed capability (implant), for instance by abusing trusted communications such as the VPN, often by "hiding in normal outbound and inbound traffic, hijacking existing communications".
- *Act*: can consist of many different actions; common activities include: discovery (and corruption) of new targets (application systems or data); "lateral movement around the network"; "installation and execution of additional capabilities"; data exfiltration; "anti-forensic techniques, such as cleaning traces of the attack activity"; and defending implant's or attacker's foothold when encountering defences or incident responders.
- *Attack* Development and Tuning: the attacker develops capabilities tailored to the specific target and for the aimed results.
- *Testing*: consists in testing the developed capabilities against a testing facility as similar as possible to the target environment, often based on information gathered in the previous steps.
- *Delivery*: consists in the delivery of the newly developed capabilities specific to the aimed target.
- Installation: is the installation (or modification) of the old software with new specific software capabilities.
- *Execution*: consists in running the software weapon to achieve the desired results.

The premise of this model is that "just one mitigation breaks the chain and thwarts the adversary. Therefore, any repetition by the adversary is a liability that defenders must recognize and leverage" (HUTCHINS; CLOPPERT; AMIN, 2010). APTs are usually well succeeded because defences are often based on pattern matching, and only able to

recognize events of some of the stages individually, but not the entire attack.

Backdoors

Implants can be inserted into software as it is being developed, and can be used for creating remotely operated *kill switches* and *backdoors* written into the computer chips' firmware allowing outsiders to remotely manipulate the systems they run.

Already in 2001, U.S. intelligence officials believed "that certain hardware and software imported from Russia, China, Israel, India, and France" were infected with *devices* able to "read data or destroy systems", although the suspicion was hard to verify (ADAMS, 2001).

Recently, however, counterfeit hardware has been identified in systems procured by the U.S. DoD (LYNN, 2010). A U.S. House Permanent Select Committee on Intelligence report, in 2012, posed recommendations restricting the acquisition of networking equipment from Chinese companies Huawei and ZTE (BANACH, 2012). In December of 2015 Juniper Networks announced the discovery of a secret backdoor in the operating system of their firewalls (ZETTER, 2015). It has not become clear who did put that backdoor in the system.

Intelligent Agents

APTs are perhaps the most sophisticated type of software weapons. The most famous one up to date is Stuxnet, which amongst many features it had is also "noteworthy for something it did not do": although an intelligent agent, it was not a *learning* agent. Machine-learning techniques are quickly developing, and a next generation agent could be able to *learn*. Indeed, as the "defence and intelligence establishments in the United States, Britain and Israel have traditionally been well ahead of general trends in computer science research", it "would be surprising if an intelligent coded weapon capable of learning had not been developed yet" (RID; MCBURNEY, 2012).

The same rationale on learning agents applies to defence systems. Back in 2009, the U.S. Department of Homeland Security published A Roadmap for Cybersecurity Research where it appointed the need for threat detection based on machine learning mechanisms to find outliers (ESTADOS UNIDOS, 2009, p. 39). This is usually called *active defence*.

Asymmetry

The term *asymmetrical warfare* is sometimes used to characterize "countering an adversary's strengths by focusing on its weaknesses" (ADAMS, 2001). It fits well in the idea of "no forced entry in cyberspace", but simply the exploitation of the enemy's vulnerabilities (LIBICKI, 2009, p. iii e xiv).

However, focusing on the adversary's weaknesses would be wise in any conflict, not only in asymmetrical ones. The best definition, so, is that which considers *asymmetry* as the disparity between the powers of the opponents.

The costs of developing conventional or nuclear forces exert a dissuasion effect, by the futility of competing with the U.S. Navy in constructing carrier task forces and submarine fleets, for instance (NYE, 2012; RUMSFELD, 2002). The same idea applies to the development of missile defences. Besides the costs, there are the difficulties associated with the access to related technologies, as the seamless rocket tubes made of special alloys, needed for missile production, and the components required for the manufacture and operation of small nuclear reactors for carriers and submarines.

It is not difficult to imagine that a Stuxnet-like tool could be used to infect and disable missile defences of the U.S., Russia, China, India or Pakistan, for example. As Stuxnet has damaged the mechanical parts of the Iranian centrifuges, the same effect could be achieved in the steam turbines of nuclear subs. Alternatively, this worm could perhaps damage some mechanical component, preferably of difficult replacement, of missiles' launching platforms. In these hypothetical ways, a tool whose cost would be in the tenths of millions would have disabled missile defences billions of dollars. Perhaps not even a worm would be necessary; just a backdoor could cripple the missile alert or launching systems for, say, half an hour.

This is the scenario usually associated with the concept of asymmetry related to Software Power, since "the barriers to entry in the cyber domain are so low that non-state actors and small states can play a significant role at low cost" (NYE, 2012).

> The asymmetry is also created by the imbalance of attack space – larger, technologically dependent nations possess a larger network space with a greater number of weak spots vulnerable to attacks, while the smaller nation has a smaller network surface to protect (ARENG, 2014).

This turns into a situation where, even though great powers make larger investments in the development of cyber capabilities, small states still have more opportunity to compete in this domain than in traditional warfare, because "in modern warfare, 'mass' is no longer a decisive factor", and "asymmetric warfare dilute the traditional power and dominance logic" (ARENG, 2014).

> More to the point, it is precisely because others suffer inferiority in conventional conflict that they feel driven to emphasize cyberattacks as a way to even the score. Thus, the United States, for all its advantages, might suffer more than adversaries would if retaliation begets counterretaliation (LIBICKI, 2009, p. 32).

Software power, so, offers means for "Lilliputian States" (as also non-state actors) to develop their capabilities and face opponents that otherwise could not be confronted (ARENG, 2014). In defence terms, this has been captured by the World Economic Forum's 2015 Network Readiness Index, which showed no G20 countries in the top five positions, occupied by Singapore, Finland, Sweden, Netherlands, and Norway respectively (AUSTIN, 2016a).

Ephemeral Nature

The entire concept of cyber attack tools is based on the exploitation of vulnerabilities. It can be by means of the *weaponization* of an Adobe PDF or Microsoft Word file with malicious code, or possibly thru the exploitation of a backdoor installed in a network asset, like a router. However, when a vulnerability is reported to the software manufacturer, it releases *patches* to fix it. The same situation happens with Intrusion Detection Systems and anti-virus software. When the patch is applied that specific vulnerability becomes useless for that particular target, and another one needs to be found.

Clearly, an exploitation may have already occurred when the patch is applied, and an implant may have been already installed. However, supposing this implant has been designed to exfiltrate data by establishing a VPN, for instance, using privileges of a stolen user id and password, that password could be changed, ceasing the possibility of that implant to execute its mission.

Moreover, as long as long as this implant tries to use the now

invalid credentials, it would reveal itself to the defenders monitoring the network, allowing further attribution and its undesired effects. To avoid this situation, the implant may be intelligent enough to detect that the credentials are not valid and "commit suicide", deleting itself to eliminate its traces and avoid forensics.

In any case, attacking tools are valid for a very specific scenario of vulnerabilities present in a particular combination of versions of the software: application, operating system, IDS and anti-virus, and their patches. An un-patched version of the operating system may be protected by the latest version of the anti-virus, and so on.

Unpredictable and Uncontrollable Propagation

Cyber weapons are also integral to the globally interconnected cyberspace in which we are immersed. "The effects of attacks at one point can spread unpredictably, far beyond the target and even back to the attacker, given *the highly interdependent nature of cyberspace*." (MORGAN, 2010)

One of the interesting aspects of Stuxnet is the fact that it infected an air-gapped network, or a system not connected to the Internet, indicating that it has possibly got its target thru a vast range of technical components, from an infected USB drive to off-the-shelf software or hardware components, as a plug-and-play driver or whatsoever (ARQUILLA, 2011).

The development of software weapons faces a tricky dilemma: should the aims be wide-and-shallow or narrow-and-deep? Essentially, achieving greater destructive potential will likely to significantly increase the development and deployment complexity, thus cost and time, while limiting potential targets, the risk of collateral damage and, hence, the political utility of the weapon (RID; MCBURNEY, 2012).

For some time it has been speculated that a programming error allowed Stuxnet to "escape" beyond the confines of its initial target's networks. Currently, however, it is believed that its original mission, the destruction of the Iranian nuclear centrifuges, have been changed in a later version, allowing it to realize reconnaissance tasks, sending to its creators the IP addresses of machines infected by contractors working for the Iranians. The more "aggressive programming features" implemented in Stuxnet latest versions would have also increased the chances of it being discovered, as indeed it was in June 2010 by a small security company in Belarus (HARRIS, 2014, p. 46-47). "Escaped" or not it has

infected many information systems in more than 150 countries, and now it may be reengineered for other purposes (ARQUILLA, 2011). This is, indeed, an important "feature" of cyber weapons: its fast and uncontrolled proliferation. Langner even celebrated the fact that Stuxnet had been developed by the U.S.; the different levels of control implemented in it avoided a major strike on Industrial Control Systems using the same (or similar) targeted Siemens software worldwide (LANGNER, 2011).

U.S. Dominance (or the Software Superpower)

During the Cold War, when the world was divided in two, Brodie defined the U.S. as a status quo nation: "determined to keep what it has, including existence in a world of which half or more is friendly or at least not sharply and perennially hostile" (BRODIE, 1959).

After the disintegration of the USSR, the U.S. has become an uncontested superpower in both conventional and nuclear force. Nowadays, it is still a status quo nation, but not with only a half of the world. Indeed,

> [...] American leaders from both the Democratic and Republican parties have made it clear that they believe the United States, to quote Madeleine Albright, is the "indispensable nation" and therefore it has both the right and the responsibility to police the entire globe (MEARSHEIMER, 2010).

The U.S. software industry is the largest in the world, being a net exporter and concentrating many of the best code writers of the world; its universities' computer science courses are top ranked, and the Pentagon is already working in public-private partnerships for creating superior military capabilities in the cyberspace (LIBICKI, 2009; LYNN, 2010; MORGAN, 2010; RID; MCBURNEY, 2012). Although there is considerable secrecy regarding U.S. attack capabilities, it is widely believed that U.S. cyber military capabilities are the best in the world.

The U.S. has just increased by 35% ($19 billion dollars) its budget for cyber security policies, including $3 billion for the creation of its new Cyber Reserve (AUSTIN, 2016a). It views supremacy in the "fifth domain" as essential to its mission, and has incorporated cyber attacks into conventional warfare. It has used them to disable infrastructure in other countries

in the same way they say to fear domestically (HARRIS, 2014, p. xxi).

Recently leaked Presidential Policy Directive 20 (PPD-20) "instructs the military to draw up a list of overseas targets "of national importance" where it would be easier or more effective for the United States to attack with a cyber weapon than a conventional one" (HARRIS, 2014, p. 54; ESTADOS UNIDOS, 2012). "On the spectrum of cyber hostilities, the United States sits at the aggressive end" (HARRIS, 2014, p. xxi). The best evidence is Stuxnet and Snowden cases.

CONCLUSION

A thorough analysis of the available literature on cyber power and cyber deterrence, mostly written by authors from NATO partners, shows that it reflects an aggressive posture, based on the need of attacking tools that could both instil fear and impose dominance in the cyberspace. Moreover, the evidence presented by both Snowden and Stuxnet cases, as also Nitro Zeus, as that of the other cases analysed, support this perception.

So far, a few acts of coercion thru sabotage, but many reported cases of espionage, with the threat of influence on decision making. In other words, coercion. Dominant state actors so far are the members of the Five Eyes group (U.S., UK, Australia, Canada and New Zealand), and North Korea, India, Israel, Iran, and France, often cited in the active pole of cyber offences.

In the globalized economy of these days, every nation might have interests that conflict with at least one of the cited countries. Thus there is the need of protecting them accordingly. This requires long-term preparation, planning, and investments, typical on matters of national security and defence.

The good news is there are excellent commercial opportunities in the market of defence *Software Power* that can be explored by non-aggressive nations while they develop their defences.

ATAQUES CIBERNÉTICOS PATROCINADOS PELO ESTADO

RESUMO

Nas sociedades pós-industriais computadores são ubíquitos e pervasivos. Adicionalmente, são interconectados. Enquanto essas características atribuem produtividade sem precedentes, elas também apresentam riscos nunca antes enfrentados. Ofensas cibernéticas introduzem a ameaça de que nações poderosas, tanto na expressão militar quanto naquela econômica, sejam confrontadas por estados muito mais fracos, ou ainda por protoestados ou grupos terroristas. Ao mesmo tempo, superpotências cibernéticas desenvolvem a habilidade de remota e subrepticiamente coagir oponentes sem a necessidade de empregar tropas no teatro de operações tradicional. Este artigo delineia as ameaças postas por ofensas cibernéticas patrocinadas por estados e analisa suas características, descrevendo suas aplicações à luz de alguns conceitos militares tradicionais, bem como suas motivações, a natureza de suas operações, dos *guerreiros* e das *armas* usadas.
Palavras-chave: Ciberespaço. Ofensas. Projeção de poder. Negação de área. Software Power.

REFERENCES

ADAMS, J. Virtual Defense. *Foreign Affairs*, v. 80, n. 3, p. 98, 2001.

ARENG, Liina. *Lilliputian states in digital affairs and cyber security.* Tallin: CCDCOE, 2014. Tallin Paper, n.4. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf>. Acesso em: 16 fev. 2016.

ARQUILLA, John; RONFELDT, D. Cyberwar is coming! *Comparative Strategy*, v. 12, n. 2, p. 141–165, 1993.

ARQUILLA, John. From blitzkrieg to bitskrieg: the military encounter with computers. *Communications of the ACM*, v. 54, n. 10, p. 58-65, Oct. 2011.

ASSANTE, M. J.; LEE, R. M. *The industrial control system cyber kill chain.* [s.l.]: SANS Institute Reading Room, Oct. 2015. Disponível em: <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>. Acesso em: 7 jun. 2016.

AUSTIN, G. Middle powers and cyber-enabled warfare: the imperative of collective security. In: ASIAN SECURITY CONFERENCE - SECURING CYBERSPACE: ASIAN AND INTERNATIONAL PERSPECTIVES, 18., 2016, New Delhi. *Anais*... New Delhi: IDSA, Feb. 2016a

_____. Strategic culture and cyberspace: Cyber militias in peacetime?. *The Diplomat Magazine*, Tokyo, 12 Feb. 2016b. Disponível em: <http://the-diplomat.com/2016/02/strategic-culture-and-cyberspace-cyber-militias-in-peacetime/>. Acesso em: 16 fev. 2016.

BANACH, W. *Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE*. Washington: U.S. House of Representatives, 8 Oct. 2012. Disponível em: <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf>. Acesso em: 12 jun. 2016.

BETZ, D.; STEVENS, T. *Cyberspace and the state*: towards a strategy for cyber-power. London, U.K: Routledge for the International Institute for Strategic Studies (IISS), 2011.

BRODIE, B. The anatomy of deterrence. *World Politics*, v. 11, n. 02, p. 173–191, jan. 1959.

BUCHANAN, B. *The Cybersecurity dilemma*: Hacking, trust and fear between nations. United Kingdom: C Hurst & Co Publishers, 2017.

CAMPBELL, D. *Development of Surveillance Technology and Risk of Abuse of Economic Information* Part 2/5. Brussels: European Parliament, 1999. Disponível em: <http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf>. Acesso em: 26 set. 2016.

CILLUFFO, F.; CARDASH, S.; SALMOIRAGHI, G. A blueprint for cyber deterrence: building stability through strenght. *Military and Strategic Affairs*, v. 4, n. 3, p. 3–23, 2012.

CLARKE, R. A.; KNAKE, R. K. *Cyber war*: the next threat to national security and what to do about it. New York: HarperCollins Publishers, 2010.

DAVIS, P. Deterrence, influence, cyber attack and cyberwar. *International Law and Politics*, v. 47, n. 327, p. 327–355, 2015.

DENNING, D. Rethinking the cyber domain and deterrence. *Joint Forces Quarterly*, v. 77, n. 2nd Quarter, p. 8–15, 2015.

EQUIPMENT interference code of practice: pursuant to section 71 of the regulation of Investigatory powers act 2000. London: TSO, 28 Jan. 2016. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf>. Acesso em: 6 jun. 2016.

ESTADOS UNIDOS. Department of Homeland Security. *A roadmap for cybersecurity research*. Washington: US Department of Homeland Security, Nov. 2009. Disponível em: <https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>. Acesso em: 8 dez. 2016.

ESTADOS UNIDOS. Joint Chiefs of Staff. *JP 3-12 (R) cyberspace operations.* Washington: Joint Chiefs of Staff, 2013. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>. Acesso em: 16 fev. 2016.

ESTADOS UNIDOS. White House. *Presidential Policy Directive/PPD-20.* Oct. 2012. Disponível em: <https://fas.org/irp/offdocs/ppd/ppd-20.pdf>. Acesso em: 14 fev. 2016.

FALLIERE, N.; O MURCHU, L.; CHIEN, E. *W32.Stuxnet Dossier.* [s.l.]: Symantec, Feb. 2011. Version 1.4. Disponível em: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Acesso em: 7 dez. 2015.

FREEDMAN, L. *Strategy*: a history. United States: Oxford University Press, 2015.

GCHQ certifies six more masters' degrees in Cyber security. *GCHQ*, 23 May 2016.

GERMAN intelligence services 'alarmed' about potential Russian interference in elections. *DW.COM*, Deutsche Welle, 16 nov. 2016. Disponível em: <http://www.dw.com/en/german-intelligence-services-alarmed--about-potential-russian-interference-in-elections/a-36413582>. Acesso em: 17 nov. 2016.

GOVCERT.CH. *APT case RUAG*: technical report. [s.l.]: MELANI, 23 May 2016. Disponível em: <https://www.melani.admin.ch/dam/melani/it/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf>. Acesso em: 6 jun. 2016.

GREENWALD, G. *No place to hide*: Edward Snowden, the NSA and the surveillance state. United Kingdom: Hamish Hamilton, 2014.

HARE, F. The significance of attribution to cyberspace coercion: a political perspective. INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON), 4., 2012. *Anais...* Tallin: IEEE, 5 jun. 2012.

HARRIS, S. *@War*: the rise of the military-internet complex. United States: Eamon Dolan/Houghton Mifflin Harcourt, 2014.

HIMR Data Mining Research Problem Book. [s.l.]: GCHQ, 20 Sept. 2011. Disponível em: <https://fveydocs.org/document/hmr-data-mining/>. Acesso em: 3 mar. 2016.

HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.* Bethesda: Lockheed Martin Corporation, 2010. Disponível em: <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>. Acesso em: 26 nov. 2015.

KEDMEY, D. Report: NSA authorized to spy on 193 countries. *Time*, 1 July. 2014.

KHANDELWAL, S. U.S. Supreme court allows the FBI to hack any computer in the world. *The Hacker News*, 28 Apr. 2016.

KISSINGER, H. *World order.* United States: Penguin Group (USA), 2014.

KOPP, C. The four strategies of information warfare and their applications. *IO Journal*, v. 1, n. 4, p. 28–33, Feb. 2010.

KREVER, M.; SMITH-SPARK, L. Lavrov denies Russian influence over US election. CNN, 12 Oct. 2016.

LANGNER, R. *Cracking Stuxnet, a 21st-century cyber weapon*. TED Talks, 29 Mar. 2011. Disponível em: <https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en>. Acesso em: 12 set. 2015

LIBICKI, M. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: Rand Corp, 2009.

_____. Cyberspace is not a Warfighting Domain. I/S: *A Journal of Law and Policy for the Information Society*, v. 8, n. 2, p. 321–336, 2012.

_____. Pulling Punches in Cyberspace. In: National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. *Proceedings of a workshop on deterring cyberattacks*, Washington, D.C: National Academies Press, 2010. p. 123–147.

LIFF, A. P. Cyberwar: a new "absolute weapon"? the proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, v. 35, n. 3, p. 401–428, June. 2012.

LORD, Kristin M.; SHARP, Travis (Ed.). *America's Cyber Future: Security and Prosperity in the Information Age*. Washington, D.C: CNAS, June, 2011. v. 1. Disponível em: <http://www.cnas.org/sites/default/files/publications--pdf/CNAS_Cyber_Volume%20II_2.pdf>. Acesso em: 2 fev. 2016.

LYNN, W. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, v. 89, n. 5, Sept. 2010.

MALAGUTTI, M. *Cybersecurity in pratice (part.I)*: software power. Strife Blog, 2 Nov. 2016a. Disponível em: <http://www.strifeblog.org/2016/11/02/cybersecurity-in-practice-part-i-software-power/>. Acesso em: 2 nov. 2016.

_____. O papel da dissuasão no tocante a ofensas cibernéticas. *Doutrina Militar Terrestre em Revista*, v. 9, p. 18–27, July 2016b.

MEARSHEIMER, J. J. The gathering storm: China's challenge to US power in Asia. *The Chinese Journal of International Politics*, v. 3, n. 4, p. 381–396, 1 Dec. 2010.

MORGAN, P. M. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. In: National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. *Proceedings of a workshop on deterring cyberattacks*. Washington, D.C: National Academies Press, 2010. p. 55 – 76.

MURDOCK, J. Cyber-espionage: norway's intelligence chief accuses china of stealing military secrets. Technology, 1 Mar. 2016.

NYE, Joseph. *Cyber war and peace*. Project Syndicate, 10 Apr. 2012. Disponível em: <http://www.project-syndicate.org/commentary/cyber-war-and-peace>. Acesso em: 9 jan. 2016.

OMAND, David. *Understanding digital intelligence and the norms that might govern it*. Centre for International Governance Innovation and Chatham House, Canada, Mar. 2015. Paper Series, n. 8. Disponível em: <https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf>. Acesso em: 10 mar. 2016.

OPERATIONAL case for bulk powers. GOV.UK, mar. 2016. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf>. Acesso em: 3 mar. 2016.

OUR history. GCHQ, [201-?]. Disponível em: <http://www.gchq.gov.uk/history/Pages/index.aspx>. Acesso em: 10 mar. 2016.

PALETTA, D. U.S. Blames Russia for recent hacks. *The Wall Street Journal*, 7 Oct. 2016.

PERLROTH, N.; CORKERY, M. North Korea linked to digital attacks on global banks. *The New York Times*, 27 May 2016.

RID, T. Cyber war will not take place. *Journal of Strategic Studies*, v. 35, n. 1, p. 5–32, Feb. 2012.

RID, T.; BUCHANAN, B. Attributing Cyber attacks. *Journal of Strategic Studies*, v. 38, n. 1-2, p. 4–37, 23 Dec. 2014.

RID, T.; MCBURNEY, P. Cyber-Weapons. *The RUSI Journal*, v. 157, n. 1, p. 6–13, Feb. 2012.

RUMSFELD, D. H. Transforming the military. *Foreign Affairs*, v. 81, n. 3, p. 20, 2002.

RUSSELL, A. Strategic anti-access/area denial in cyberspace. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT: ARCHITECTURES IN CYBERSPACE, 7., 2015. *Anais...* Tallinn: NATO/CCDCOE, 2015. Disponível em: <https://ccdcoe.org/cycon/2015/proceedings/11_russell.pdf>. Acesso em: 8 jun. 2016.

SANGER, D. E. Obama ordered wave of Cyberattacks against Iran. *Middle East*, 1 June. 2012.

SANGER, D. E.; MAZZETTI, M. U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. *Middle East*, 17 Feb. 2016.

SCHNEIER, B. Computer network exploitation vs. computer network attack. *Schneier on Security*, 10 Mar. 2014. Disponível em: <https://www.schneier.com/blog/archives/2014/03/computer_networ.html>. Acesso em: 28 nov. 2015

SHALAL, A. U.S. National guard may join cyber offense against Islamic state: Carter. *Reuters*, 6 Mar. 2016.

SHARMA, A. Cyber wars: A paradigm shift from means to ends. *Strategic Analysis*, v. 34, n. 1, p. 62–73, 5 Feb. 2010.

SINGH, S. *The code book*: the science of secrecy from ancient Egypt to quantum Cryptography. United States: Knopf Doubleday Publishing Group, 2000.

STOLL, C. *The cuckoo's egg*: tracking a spy through a maze of computer espionage. London: The Bodley Head, London, 1990.

STONE, J. Cyber war will take place! *Journal of Strategic Studies*, v. 36, n. 1, p. 101–108, Feb. 2013.

_____. Technology and war: a trinitarian analysis. *Defense & Security Analysis*, v. 23, n. 1, p. 27–40, Mar. 2007.

SWIRE, P. *US surveillance law, safe harbor, and reforms since 2013.* [s.l: s.n.]. 2015. Disponível em: <https://fpf.org/wp-content/uploads/2015/12/White--Paper-Swire-US-EU-Surveillance.pdf>. Acesso em: 3 mar. 2016.

WAGSTYL, S. German security head warns of election interference from Russia. *Financial Times*, 16 Nov. 2016b.

_____. Germany points finger at Kremlin for cyber attack on the Bundestag. *Financial Times*, 13 May 2016a.

YADRON, D. Supreme court grants FBI massive expansion of powers to hack computers. *The Guardian*, 3 May 2016.

ZETTER, K. Everything We Know About Ukraine's Power Plant Hack. *WIRED*, 20 Jan. 2016.

_____. How digital detectives deciphered stuxnet, the most menacing malware in history. *WIRED*, 11 July 2011.

_____. Secret code found in juniper's firewalls shows risk of government backdoors. WIRED, 18 Dec. 2015.

Recebido em: 22/09/2016
Aceito em: 09/12/2016