DOI 10.21544/1809-3191.v25n1.p89-128

THE CONVERGENCE OF CYBER, ELETRONIC AND KINETIC WARFARE WITHIN THE SCOPE OF SEA POWER

Alan Oliveira de Sá[1]
Raphael Carlos Santos Machado[2]
Nival Nunes Almeida[3]

ABSTRACT

The search for increasing Sea Power operational and management capabilities has promoted the use of hybrid systems, in which cyber components interact with physical plants and with sensors/devices that explore the electromagnetic spectrum. However, at the same time as this integration brings benefits, it also exposes such systems to new threats resulting from the encounter of cyberwarfare with electronic and kinetic warfare. This study analyzes how these new threats can affect Sea Power, characterizing, through examples, their possible targets. To support this discussion, we propose a taxonomy encompassing new classes of attack that exploit the cyber, electronic and kinetic domains. Our analysis indicates the need for policies capable of promoting Sea Power cyber security. In this sense, we discuss policies on personnel training and certification of cyber products, both of them having the potential to contribute extensively to Sea Power security.

Keywords: Cyberwarfare. Electronic Warfare. Kinetic Warfare. Sea Power.

[1] Professor at the Admiral Wandenkolk Instruction Center (CIAW), Rio de Janeiro (RJ), Brazil. E-mail: alan.oliveira.sa@gmail.com / ORCID: http://orcid.org/0000-0001-6311-9672

[2] Professor at the Federal Fluminense University (UFF), Rio de Janeiro (RJ), Brazil. E-mail: rcmachado@inmetro.gov.br

[3] PhD at the Naval Warfare School (EGN), Rio de Janeiro (RJ), Brazil. E-mail: nivalnunes@yahoo.com.br

INTRODUCTION

The inclusion of cyber domain[4] in the art of war has been widely discussed in the fields of Science and Technology, Defense, Strategy and International Relations. Due to their complexity and peculiarities, cyber threats have led researchers and strategists to review the long-established principles of war derived from the works of Sun Tzu, Nicolas Machiavelli, Carl von Clausewitz, Antoine-Henri Jomini, Basil Liddell Hart, among others. Such principles, originally formulated considering millennia of kinetic warfare5, are not fully suited to the warfare practiced in the cyber domain. According to Parks and Duggan's assessment (PARKS; DUGGAN, 2011), among the principles of kinetic warfare (WEIGLEY, 2013; MINISTRY OF DEFENSE, 2007; MINISTRY OF DEFENSE, 2014), there are those that apply to cyberwarfare, those which have no meaning in cyberwarfare and a few that can indeed be considered antagonistic to cyberwarfare. However, from the earliest kinetic war strategists and theorists to the current cyberwarfare researchers, a common feature can be observed in both types of warfare. Both must have a real-world effect.

Among the eight principles proposed by Parks and Duggan, in cyberwarfare such a feature is explicit in the principle of Kinetic Effects. This principle states that cyberwarfare must have effect in the kinetic world; it is meaningless unless it affects someone or something in the real world. In other words, we can say that the energy expended by cyber warriors in combat only results in work when the results affect - directly or indirectly - the physical world.

Despite difficulties in discovering and scrutinizing cyberwarfare attacks – which are sometimes kept secret - the principle of Kinetic Effects is often identified in the cases studied. Among the most well-known attacks, whose produced/alleged effects underscore this relevance of this principle, we point out the attack associated with the explosion in the Trans-Siberian pipeline (REED, 2005; CLARKE; KNAKE, 2010), the cyber

[4] The concept of cyber domain adopted in this article is based on the definition of cyber world presented by Parks and Duggan (PARKS; DUGGAN, 2011). According to those authors, a cyber world is "any virtual reality contained in a collection of computers and networks." Note that this definition assumes the existence of several cyber worlds, of which the Internet would be the most relevant. Therefore, the term cyber domain is used in this article to represent the set of all existing cyber worlds.

[5] In the definition presented by Parks and Duggan (PARKS; DUGGAN, 2011), also adopted in this article, the term kinetic warfare refers to warfare practiced in the land, sea, air and space domains. It is the warfare involving tanks, ships, aircraft, soldiers etc.

attack that supported Operation Orchard (ADEE, 2008; CLARKE; KNAKE, 2010; DIPERT, 2013) and the Stuxnet worm (LANGNER, 2011; ZETTER, 2014) that impacted the Iranian nuclear program.

The three cases are examples of attacks in which real-world effects gave attackers - nation states, according to CLARKE and KNAKE (2010) and ZETTER (2014) - tactical or strategic advantages, either by inflicting direct physical harm on the enemy or by interfering with tactical information in the theater of operations. Such examples highlight the need to understand the forms the principle of Kinetic Effects assume in order to establish countermeasures - whether political or technical. This has motivated studies of cyber security in various contexts, especially those involving critical infrastructure6, which inevitably include Naval Power7. In fact, depending on the circumstances, an incident - cyber or otherwise - affecting a naval system (civil or military) may have negative impacts on transportation, energy, defense, food and other industries, likely producing economic, environmental and security losses.

In this context, this study discusses some ways in which attacks involving cyber components can achieve Kinetic Effects, affecting, for example, naval combat, navigation or even the exploration/use of sea and inland waters. More specifically, we discuss how Kinetic Effects can be achieved when cyberwarfare encounters two other types of warfare commonly practiced in the naval environment - electronic warfare and kinetic warfare. Therefore, our analysis considers attacks in three domains: cyber domain; the electronic domain; and the kinetic domain.

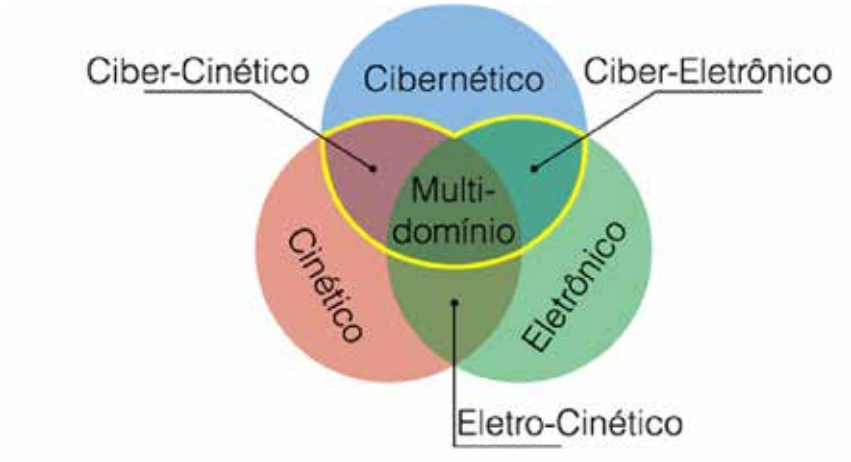
---

[6] According to Mandarino Junior (2010), critical infrastructure (CI) are "facilities, services, goods and systems whose disruption or destruction, in whole or in part, would cause a serious social, economic, political, environmental or international impact or seriously affect the security of the state and society."Among the critical infrastructures of a country we can mention, for example, those of Energy, Defense, Transport, Telecommunications and Finance, among others (WHITE HOUSE, 2003; MANDARINO JUNIOR, 2010).

[7] We adopted in our study the concept of Sea Power established in the Brazilian Basic Navy Doctrine (MARINHA DO BRASIL, 2014): *"Sea Power is the capability resulting from the integration of the resources available to the Nation for the use of the sea and inland waters, either as an instrument of political and military action, or as an economic and social development factor."* According to this doctrine, sea power consists of the following elements: *"Naval Power; the Merchant Marine, facilities, services and organizations related to water transportation (in both maritime and inland waters); water transportation infrastructure: ports, terminals, locks and support and control means and facilities; the shipbuilding industry: construction and repair yards; the defense industry of interest to the shipbuilding sector; the fishing industry: vessels, terminals and fish processing facilities; the technological research and development organizations and means related to the use of the sea, inland waters and their resources; the organizations and means for exploiting sea resources, the seabed and its subsoil; and the personnel engaged in activities related to the sea or inland waters and the institutions for their training".*

More precisely, the focus of this study is the attack subsets shown in the intersections highlighted in Figure 1.

Figure 1 - Classification of attacks by their domains of influence/impact.



This study is divided as follows. First, we describe some relevant cyber attacks that have already occurred, as well as their real-world impacts. Next, we present a taxonomy covering attacks directed to the cyber, electronic and kinetic domains. This taxonomy aims to support the discussion of possible attacks involving these three domains. Subsequently, the study discusses the classes of cyber-kinetic, cyber-electronic and multi-domain attacks, characterizing, with examples, their possible targets involving the Naval Power. Next, we discuss policies with the potential to mitigate such attacks. Finally, the conclusions are presented.

CYBERWARFARE ACTIONS

Until now, humanity has not experienced cyberwarfare as extensively as kinetic warfare. While, on the one hand, knowledge about kinetic warfare was built on thousands of years of observations and records, on the other hand, cyberwarfare concepts are based on a few decades' experience. Nevertheless, cyber attacks already carried out represent a valuable source of information for the study of cyberwarfare and its developments. This section thus presents examples of cyberwarfare

attacks with different purposes and forms of deployment. Although the attacks described here have not been carried out in naval areas - that is, against navy ships, civilian vessels or infrastructures on the shore or under or above the water surface - they generally serve as a reference or proof of concept for possible attacks that may cause incidents in naval jurisdictions.

ATTACK ON ESTONIA

In 2007, Estonia was the target of a series of cyber attacks that significantly affected the country's essential services. To understand the motivation of the attacks, it is necessary to return to the end of World War II. With the Great Patriotic War[8], the Red Army put an end to Nazi rule in Estonia, forcing it to join the Union of Soviet Socialist Republics (USSR). After the Soviet period, with the disintegration of the USSR, Estonia became independent and again established its capital in Tallinn. During Soviet rule, so that the peoples of Eastern Europe would remember the sacrifices made to free them from the Nazis, the USSR erected in many capitals of the region large statues of a heroic Red Army soldier. One of those was erected in Tallinn.

These statues were highly appreciated by Soviet leaders. However, for Estonians, the statue erected in Tallinn was a symbol of the five decades of oppression they endured as part of the USSR (CLARKE; KNAKE, 2010). Thus, in 2007, taking into account the sentiments of the population, the Estonian legislature passed the Law on Forbidden Structures which required the removal of the statue of the Red Army soldier, displeasing Moscow. To prevent incidents, the Estonian president vetoed the law. In this context, the tension surrounding the preservation or relocation of the Soviet symbol mounted.

On the one hand, Estonian public opinion advocated the removal of the statue and a nationalist group was trying to destroy it. On the other, Russian ethnic groups devoted to its protection became increasingly active. The conflict culminated in a revolt known as the Bronze Night (KAISER, 2015), which followed the removal of the statue to a military cemetery. That was when the conflict migrated to cyberspace. Estonia was hit by a large-scale DDoS attack[9] - by far the largest recorded until then.

[8] The term used by Russians to refer to World War II.

[9] In the context of Internet services, a Denial of Service (DoS) attack is a type of attack in

The attack, launched by several botnets10, lasted for weeks and toppled government electronic services, banks, newspaper websites and telephone network servers. Due to its large impact, the Baltic country took the case to NATO's North Atlantic Council. Estonia claimed that the computers controlling the botnets were located in Russia, which in turn denied being involved in the cyber attacks (CLARKE; KNAKE, 2010).

RUSSO-GEORGIAN WAR

Another known cyber attack - also involving a former Soviet republic - occurred in 2008 in Georgia (SHAKARIAN, 2011) during the Russo-Georgian War. At the time, South Ossetia was internationally recognized as Georgian territory, but it considered itself an independent republic and received Russian protection and funding, living under Russia's influence (CLARKE; KNAKE, 2010). That year, South Ossetian rebels organized a series of missile attacks on Georgian villages. In response, Georgia bombed the capital of South Ossetia and invaded the region. The day after the Georgian invasion, the Russian army responded by expelling Georgian troops from South Ossetia. It turned out that the physical offensive was not the only one launched against Georgia.

Before the kinetic attacks began, cyber attacks were already hitting Georgian government websites. Throughout the conflict, Georgia suffered DDoS attacks on its media to make it difficult for Georgians to realize what was happening. Banking, credit card and mobile phone systems were affected. Most routers connecting Georgia to the Internet via Turkey and Russia were also attacked. Georgia lost access to external sources of information and news. At the height of the offensive, six botnets were mobilized to generate attack traffic (CLARKE; KNAKE, 2010). Although some experts consider that the coordination between cyber and kinetic attacks was poor (SHAKARIAN, 2011), and Russia's claim that the cyber attacks were not commanded by the Kremlin (CLARKE; KNAKE, 2010), some events identified then suggested such a coordination. The physical

which the service run by a particular server is interrupted due to a number of requests exceeding its processing and response capacity. A Distributed Denial of Service (DDoS) attack, in turn, is a DoS attack in which a large set of equipment – consisting of up to thousands of machines - is used to generate the traffic responsible for overloading the network server and deny service. The attacking equipment, called zombies, can be computers, servers, networking equipment or even IoT devices.

[10] A network of zombie devices, or bots, remotely controlled by a master computer that in turn commands the DDoS attacks.

installations of the media and communication systems, for example, have not suffered kinetic attacks, only cyber attacks. In addition, Russian hackers attacked a website for renting diesel-powered electric generators, probably in support to the conventional attacks that hit the country's electrical infrastructure (SHAKARIAN, 2011). It is noteworthy that, according to Shakarian (2011), the objectives of isolating and silencing Georgia were limited in scope, and the attackers avoided causing permanent damage to Georgian networks and SCADA targets[11].

STUXNET

An attack on SCADA systems, with direct kinetic real-world effects, happened in a different context from the Russo-Georgian War, involving the use of - possibly - the most iconic cyber weapon ever used: the Stuxnet malware. Its strategic purpose was not the denial of internet services, but the stealth denial of nuclear weapons to Iran without resort to physical weapons. More specifically, it targeted uranium enrichment centrifuges operating at the Natanz nuclear facility. These centrifuges, which functioned in a cascade system, were controlled and operated by a SCADA system using Siemens' STEP 7 software.

Using Zetter's (2014) analogy, we can describe Stuxnet as a digital missile used to carry two types of warhead. The "missile" portion was in charge of transporting the digital warheads to the centrifuges' Programmable Logic Controllers (PLC). In other words, the "missile" part was responsible for propagating and replicating the malware - more specifically a worm - until it found a system that had the signature of the system to be attacked. Once it found the target system - Siemens CPLs connected to the centrifuges - the worm released the digital warheads into the PLCs and initiated a subtle process of degradation and destruction of the centrifuges. One of the digital warheads contained a code that altered the centrifuges' speed to reduce the efficiency of the enrichment process and caused destructive vibrations. The other warhead acted on opening and closing the valves that interconnected the cascading centrifuges, causing increased internal pressure and breakdown of the centrifuges. It is noteworthy that Iran's centrifuge control system was not directly

[11] Supervisory Control and Data Acquisition (SCADA) systems are systems used to control, monitor and acquire data from automated physical systems. The controlled physical systems range from industrial plants to critical infrastructures.

connected to the Internet, so that in order to reach the control network, the malware had to close the air gap[12] between the two networks. Thus, among other forms of dissemination, Stuxnet propagated via removable media (USB flash drives) and installed its malicious code on PLCs through the machines that were used to program them.

After the discovery of Stuxnet, research has shown that, in addition to its complexity, it had a wealth of resources never before seen together in a digital weapon. In its "missile" portion, the malware used eight forms of propagation (ZETTER, 2014), of which four were zero-day exlpoits13 (FALLIERE, 2011), which demonstrates the degree of commitment to and investment in the project.

Stuxnet was discovered in 2010 and investigated by various experts around the world (ZETTER, 2014), in the fields of industrial control systems (LANGNER, 2011) and information security (FALLIERE, 2011) alike. Evidence and investigations point to a joint US-Israel authorship (ZETTER, 2014). Stuxnet is considered a proof of concept of how digital weapons can directly affect the physical world, fulfilling the same strategic purposes of kinetic weapon attacks such as missiles and bombs.

THE ATTACK ON THE TRANS-SIBERIAN PIPELINE

Although Stuxnet is considered a milestone in attacks on cyber-physical systems, the literature on the subject (WEISS, 1996; CLARKE; KNAKE, 2010; MILLER, 2012) indicates the existence of another previous physical impact logic bomb. The weapon was said to have been used to wreak havoc on a Siberia gas pipeline in the early 1980s (CLARKE; KNAKE, 2010) - that is, even before the Internet being widespread as in Stuxnet days. At the time, without the great connectivity of the worldwide computer network, the attackers - that is, the CIA with Canadian support, according to Clarke and Knake (2010) - used another strategy to get the malicious code into the pipeline control system. They implanted the malicious code directly into the controller, even before the equipment

[12] Air gap is the term used to refer to the network security measure by which the network to be protected is physically isolated from insecure networks - such as the Internet – leaving no connectivity between them.

[13] Zero-day exploits are attacks that exploit zero-day vulnerabilities - i.e. vulnerabilities unknown to those interested in mitigating them. Zero-day vulnerabilities are rare and their exploits, when marketed in the gray or black market (ZETTER, 2014), are expensive.

was procured by Russia and installed in its pipeline automation system (CLARKE; KNAKE, 2010).

The controller would be responsible for opening and closing valves, as well as for activating the pipeline's gas pumps. Thus, according to Clarke and Knake (2010), the malicious code was programmed to command valve closure of a segment of the pipeline, while the pump operated at maximum capacity to inject gas into the pipeline. The improper functioning of the system actuators - i.e. the pump and valve - resulted in increased internal pipeline pressure, which in turn caused the largest non-nuclear explosion to date, of over three kilotons (CLARKE; KNAKE, 2010; MILLER, 2012).

OPERATION ORCHARD

A new type of attack was inaugurated with Operation Orchard, launched in 2007 by Israel against Syria. In the early hours of September 6, 2007, Israeli Air Force aircraft entered Syria's airspace and bombed an industrial facility that was being built in its territory. The facility was a nuclear plant that, according to Clarke and Knake (2010), Syria was building with North Korean support. At the time, besides the repercussion of the bombing itself and discussions about the purpose of the attacked plant, international attention was drawn to the fact that Syria, which had already invested billions of dollars in air defense systems (CLARKE; KNAKE, 2010), did not react to the attack. That night Syria was on the alert because the previous morning Israel had deployed its troops into the Golan Heights. The Syrian military closely watched their radars. However, while Israel's F-15 Eagles and F-16 Falcons invaded Syrian airspace, nothing unusual appeared on the surveillance system's radar screens.

In search of plausible explanations for the failure of the Syrian surveillance system, some analysts suggest that the country has been the victim of an electronic war attack. However, the attack differed from other known Electronic Attack Measures[14] (EAM) in exploiting a vulnerability

[14] According to the Brazilian Navy (MARINHA DO BRASIL, 2014), Electronic Attack Measures (EAM) are a *"set of actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum and also to degrade, neutralize or destroy their combat capability through equipment and weaponry using this spectrum."* EAMs are fundamentally tactical in nature and represent one of three branches of Electronic Warfare Measures (EWM) - which also encompass Electronic Protection Measures (EPM) and Electronic Warfare Support Measures (EWSM) (MARINHA DO BRASIL, 2014) .

of the Syrian surveillance system's cyber domain (ADEE, 2008; CLARKE; KNAKE, 2010).

Radar systems, like sensors, are interfaces open to the environment. To obtain information about potential targets, a radar system transmits pulses through its antenna and generally captures any echoes coming back to its receiver. The received echoes, in turn, are digitized, stored in memory and processed by a computer system that presents the operator with relevant information about the detected targets, such as positions and velocities (BOLE, 2005). Thus, a transmitter, capable of transmitting pulses in the same pattern as those transmitted by radar, is able to cause false echoes - synthetically produced – to reach the radar antenna (ABDALLA et al., NENG-JING; YI (1995). These false echoes, once digitized, are represented as bits in the radar system's memory (BOLE; DINEY; WALL, 2005). This means that it is possible to interfere with the data bits of a radar system's memory through known EAMs - which is not big news given the state of the art of electronic warfare (ABDALLA et al.; 2015). However, in this attack, it is possible that there was a hidden digital trigger in the surveillance system - a vulnerability implanted into software and/or hardware - constantly watching for information captured and saved in the radar system's memory fitting a specific pattern that would activate it (ADEE, 2008; CLARKE; KNAKE, 2010). This digital trigger, in turn, would initiate malicious routines in the radar computer system. Basically, there would be two malicious routines: a recording routine and a scenario playback routine. The information, or the bits, containing the specific trigger pattern would be fed into the system's memory by the EAM through the radar antenna itself. Once identified the triggering pattern of the recording routine, the digital trigger would start recording a normal scenario - i.e. without targets that posed threats. Later, after identifying the trigger pattern of the playback routine, the digital trigger would start to reproduce for the operators the normal scenario previously recorded during the recording routine. Thus, an EAM together with a digital trigger in the radar computer system would have prevented Syrian operators from detecting enemy aircraft during the bombing operation (CLARKE; KNAKE, 2010).

A SUMMARY OF THE ATTACKS

The cyberwarfare actions presented above are not a comprehensive list of all cyber attacks that have already taken place. Nevertheless, they demonstrate the diversity of the attacks, as well as the ways in which they were effectively used as a tool to cause physical or economic damage to opposing nations, or even to support kinetic attacks in military operations. In the case of Estonia, we highlight that only cyber attacks were carried out, impacting the real world by denying services essential to the Estonian economy and society. In the Russo-Georgian war, cyber attacks were employed to support attacks by conventional forces (SHAKARIAN, 2011), with some degree of coordination between them. In the examples of Stuxnet and the attack on the Trans-Siberian pipeline, digital weapons were employed to cause direct physical damage to the enemy without the use of conventional forces. In Operation Orchard, an attack involving cyber and electronic warfare was coordinated to support attacks by conventional forces. These examples thus show three possible types of attack:

- cyber attacks aimed at affecting information and communication systems, but not for the purpose of directly affecting physical systems (attacks on Estonia and the Russo-Georgian War);

- cyber attacks for directly affecting physical systems (Stuxnet and the attack on the Trans-Siberian pipeline); and

- cyber attacks involving EAM aimed at hampering tactical intelligence, but not for the purpose of directly interfering with physical systems (Operation Orchard attack).

An in-depth analysis of these offensives suggests the possible development of cyber attacks involving EAM that could directly affect physical systems. More specifically, in naval systems, this possibility arises from the increasing integration between computer systems, physical plants, communication systems and sensors that explore the electromagnetic spectrum (BOYES; ISBELL, 2017; LAGOUVARDOU, 2018; BHATTI; HUMPHREYS, 2017). Thus, this study focuses on offensive actions that shift among cyber, electronic and kinetic domains, with possible impacts on the naval environment.

TAXONOMY

Technology integration into combat tools and techniques has often led to periodic reviews of military taxonomy. These taxonomic reviews aim to support the discussion and study of war, as well as to establish concepts for use in the development of defense capabilities. In this sense, this section presents a taxonomy that brings together existing terminologies in the literature and establishes new terms and concepts related to attacks that exploit cyber, electronic and kinetic domains. First, it is necessary to observe the definitions of cyber, electronic and kinetic wars:

- **Cyberwarfare**, according to Parks and Duggan (PARKS; DUGGAN, 2011), is a combination of computer network attack and defense and special technical operations. The environment in which such actions occur is referred to as cyberworld, defined as "... any virtual reality contained in a collection of computers and networks." (PARKS; DUGGAN, 2011, p. 1)

It is worth of notice that the definition admits the existence of several cyberworlds, since different virtual realities contained in different unconnected collections of computers and networks may coexist. Also according to Parks and Duggan (2011), among the various existing cyberworlds, the Internet is the most relevant.

The concept of cyber domain adopted in this article is based on the definition of cyberworld presented by Parks and Duggan (2011). In this context, the cyber domain corresponds to the environment composed of all existing cyberworlds.

- **Electronic warfare**, according to Shelton (1998), corresponds to: "... any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy." (SHELTON, 1998, p.II-5).

In line with this definition, the Electronic Defense War Policy (MINISTÉRIO DA DEFESA, 2004) states that Armed Forces' electronic warfare actions generally aim to ensure the use of the electromagnetic spectrum and to prevent, reduce or prevent its use against national interests. The domain of electronic warfare, therefore, lies in the electromagnetic spectrum, more specifically in the frequency ranges in which operate sensors (for example radar systems), electronic warfare equipment and communication systems using electromagnetic waves.

- **Kinetic warfare**, according to Parks and Duggan (2011), is defined as: "...warfare practiced in the land, sea, air, and space domains. All

current militaries' tanks, ships, planes, and soldiers are kinetic warfare's protagonists." (PARKS; DUGGAN, 2011, p.1)

Note that the definition of kinetic warfare presented by Parks and Duggan (2011) does not clearly characterize a particular domain for this type of war, since cyber and electronic warfare actions can also be carried out in land, sea, air and space. Therefore, to characterize the domain of kinetic warfare, we refer to the meaning of kinetics. Considering that kinetics is the branch of physics that studies the effects of forces on the motion of bodies, we can establish that the domain of kinetic warfare is the real world - that is, not virtual – which is subject to change by applying forces.

The examples of digital offensive operations discussed earlier in this study demonstrate the existence of hybrid cyber attacks that, to produce the desired kinetic effect, also exploit the electronic and kinetic domains. In Figure 1, we highlight three classes of hybrid attacks, combining actions in the cyber domain with actions in the electronic and/or kinetic domains:

- **Cyber-Kinetic**: cyber-kinetic attacks are offensives originating in the cyber domain, with the objective of causing direct real-world impacts. Its targets are systems in which computers and communication networks are used to initiate or control physical processes. In other words, in this type of offensive, digital attack measures are employed to produce physical forces capable of directly affecting the real world.

- **Cyber-Electronic**: cyber-electronic attacks are attacks composed in part of electronic warfare actions but also containing elements of cyberwarfare. According to Yasar (2012), cyber-electronic attacks are a new and improved form of electronic attack. In a traditional electronic warfare, an EAM - for example a jamming action - can be used, for example, to deny the enemy the use of the radar's electromagnetic spectrum. On the other hand, in a cyber-electronic attack, the use of the electromagnetic spectrum by the target system is not necessarily prevented. In this case, the electromagnetic spectrum is used by the attacker to send a data stream to the target system processor to interfere with its computational process, thus compromising its operation. To this end, a cyber-electronic attack exploits, as a gateway, the same electromagnetic wave devices that the target system uses to fulfill its tactical/operational function.

- **Multi-domain**: multi-domain attacks are attacks that exploit the three domains: cyber, electronic and kinetic. They target systems that in some way interconnect physical plants, automation and control computer systems, and devices/sensors that use the electromagnetic

spectrum. In these systems, computers and networks are used to initiate or control physical processes, and which also connect to - and occasionally interact with - electronic warfare systems. Conceptually, attacks start in the electromagnetic spectrum and use as input the electromagnetic wave devices - for example the radar antenna. They are intended to interfere with or cause direct physical damage to physical plants. To achieve this, they use a cyber component as a pivot between the domains of electronic and kinetic warfare. This cyber component, a digital mechanism implanted in software and/or hardware, is responsible for transforming information received from the electromagnetic spectrum into malicious kinetic actions in the controlled plant.

In Figure 1, we can also observe a fourth subset of attacks that, by definition, act simultaneously - and exclusively - in the electronic and kinetic domains. Such attacks, which do not target the cyber domain, are not addressed in this study (which focuses on the meeting of cyberwarfare with electronic and kinetic warfare). However, for the sake of completeness of the present taxonomy, we define them as electro-kinetic attacks. We can include in this class, for example, electromagnetic offensives launched against proximity fuses used in World War II (BONNER, 1947; BROWN, 1993). Proximity fuses, embedded in projectiles, were basically made up of an electromagnetic wave transmitter and a receiver connected directly to chain of explosives (Bonner, 1947; Brown, 1993). To trigger the chain of explosives, the projectile's receiver had to just pick up the electromagnetic waves reflected by the target, which would have to meet a certain Doppler amplitude and frequency pattern. The detonation process did not go through the cyber domain. Based on the fuse architecture presented by Bonner (1947) and Brown (1993), it is possible to say that the launch of electromagnetic interference specifically against this type of fuse would be able to eventually induce projectile detonation, causing direct effects on the kinetic domain. Note that an attack against these fuses acts in both the electronic and kinetic domains without making use of the cyber domain at any time. For this reason, we classify it as an electro-kinetic attack.

It is noteworthy that, in our proposed taxonomy, the classes of cyber-kinetic, cyber-electronic and multi-domain attacks only specify the domains that are exploited during the execution of a given offensive. However, the nomenclature adopted and the examples discussed in this study do not exhaust all possible paths that an attack may take while going through the domains of its respective class.

DISCUSSION

After establishing a taxonomy encompassing cyber-kinetic, cyber-electronic and multi-domain attacks, we present in this section a discussion of the use of these attacks against Sea Power targets. First, we briefly discuss cyber-kinetic, cyber-electronic, and multi-domain attacks, and characterize some of their possible targets. We then discuss policies that can broadly contribute to mitigate these types of threats.

The examples of attacks mentioned above show that their targets are not exclusively military. While Operation Orchard's cyber-electronic attack targeted a military air surveillance system, the attacks on Estonia and Georgia mostly had civilian targets; as well as the cyber-kinetic attack on the Trans-Siberian pipeline. Therefore, we discuss here both civil and military targets. Although there are sometimes noticeable differences between these two types of targets, they often share the same technologies - often dual. In addition, an attack on either kind of target may cause significant impacts on Naval Power, Sea Power and the nation.

CYBER-KINETIC ATTACKS

According to our taxonomy, a cyber-kinetic attack aims to cause direct impacts on a physical plant by digitally interfering with the cyber domain. In this type of attack, targets typically are physical plants, computer systems, sensors, actuators and communication systems (DE SÁ; CARMO; MACHADO, 2017; LANGNER, 2011). Sensors have the role of measuring the physical functioning of the plant, while actuators transform control signals into physical actions capable of altering its state. Control signals are handled by conventional computers, microcontrollers or computers designed specifically for controlling physical processes, such as Programmable Controllers (PC) or Programmable Logic Controllers (PLC) [15]. The last two (i.e. PCs and PLCs) are widely used in most of the plant automation and control systems.

[15] PLCs and PCs are computer systems specifically designed to control/automate physical plants. In general, they are generic off-the-shelf devices that can be used to control various types of systems by programming them according to the characteristics of the plant. They consist of microprocessors, memories, programming/communication interfaces, and signal input and output interfaces. Signal input interfaces are used to receive signals measured by sensors in the plant. Signal output interfaces transmit control signals to plant actuators.

Generally, we can say that the set of potential targets for a cyber-kinetic attack comprises Internet of Things (IoT) devices (GUBBI et al., 2013), Industry 4.0 systems (LEE; BAGHERI; KAO, 2015; LASI et al., 2014) and other plant control and automation systems not necessarily industrial. Strictly speaking, with regard to Sea Power, the targets might be, for example:

- Ship automation and control systems including, for example, propulsion systems (HART, 2004) and power generation systems (ZIVI, 2005) in both merchant and naval vessels. In the case of attacks on power generating systems, we cite as proof of concept the Aurora attack experiment conducted by the Idaho National Laboratory for the US Department of Homeland Security. In the experiment, attackers cause the destruction of a 2.25MW diesel-powered generator using a virus consisting of 20 lines of code (AYALA, 2016);

- Naval combat systems, in which sensors and weapons are connected to computers and networks - even local ones - according to the examples discussed in Norcutt (2001) and Janer and Proum (2014);

- Floating dikes whose stability and buoyancy control is made via SCADA systems (TOPALOV; KOZLOV; KONDRATENKO, 2016);

- Offshore systems for oil and gas exploration, production and transportation (WADHAWAN; NEUMAN, 2015; ERICKSON et al., 2003), often controlled by SCADA systems;

- Channel and lock automation control system (AMIN et al., 2010; AMIN et al. 2013; SMITH, 2015);

- Tidal power generation plants controlled by PLCs and SCADA systems (KUMAR; MAJUMDAR; BABU, 2012);

- Automated offshore wind farms16 (SUN; HUANG; WU, 2012; FLEMING et al. 2017);

- Shipyards employing typical Industry 4.0 automation and control systems in both their industrial processes and infrastructures (ARAKAKI, 2009).

Of course, these examples do not exhaust the target possibilities for a cyber-kinetic attack on Sea Power. However, they help to present the broad range of systems subject to this type of threat.

[16] Although they are still beginning to be explored in Brazil (LUNA, 2018), a study by the National Institute for Space Research (INPE) points out that "the offshore energy potential in the Brazilian EEZ is about 12 times greater than in the continental area of the country, being thus capable to leverage Brazil's long-term sustainable development."(ORTIZ; KAMPEL, 2011)

Note that in many of the above examples, controllers (e.g. PLCs and PCs) are also connected to supervisory systems (SCADA) via communication networks. In addition, depending on the purpose of the physical plant, there may still be a physical connection between SCADA systems and other networks - which may include a physical link to the Internet.

Where there is a need for a physical connection between the control network and other networks, the literature recommends the adoption of security solutions involving, for example, firewalls, demilitarized zones (DMZ), Intrusion Detection System (IDS) and specific network architectures (STOUFFER; FALCO; SCARFONE, 2011). Of course, a simple and efficient security measure to minimize the likelihood of attacks on these types of systems is to keep the control network isolated from other networks - i.e. without physical connectivity between them. This strategy, also known as air gapping17, is commonly adopted in critical systems such as nuclear, military, etc. However, it is important to note that the use of air gapping does not ensure the full security of cyber systems. Malware can, for example, overcome the air gap using removable media, as in the case of Stuxnet (FALLIERE; MURCHU; CHIEN, 2011); or even be implanted in the system before or during commissioning, as in the case of the attack on the Trans-Siberian pipeline (CLARKE; KNAKE, 2010). Thus the need to adopt other security measures - in addition to the technical measures exemplified above - capable of mitigating possible attacks on these types of systems, isolated or not by air gap.

CYBER-ELETRONIC ATTACKS

The concept of cyber-electronic attack presented here establishes that this type of offensive brings together elements of electronic warfare and cyberwarfare. Evidently, therefore, the potential targets for this type of attack are characterized by an architecture that interconnects devices operating in the electronic and cyber domains. Typically, these targets are electromagnetic wave transmission/reception equipment and computer systems for processing the information received via the electromagnetic spectrum.

[17] Air-gapping is a network security measure used to ensure that the computer network to be protected is physically isolated from unprotected networks, such as the Internet or an insecure local area network. As there is no physical connectivity between networks, they are isolated by what is known as a conceptual air gap.

To better understand how this type of attack may occur, we provide, as an example, a brief description of the operation of a video synthetic aperture radar. In this type of radar, the echoes received by the antenna in the form of electromagnetic waves are electronically treated, converted to binary values and stored in memory for further processing. As the radar scans the search space, all valid echoes received are stored in memory, thus forming a picture of the monitored area. To reproduce the stored information, a computational process iteratively reads the data contained in memory and converts it to the radar operator (BOLE; DINELEY; WALL, 2005).

Note that just as the actual echoes of the environment are converted to bits and stored in memory, the synthetic echoes possibly transmitted by an attacker will also be converted to bits and stored in the same memory. Thus, it is possible for an attacker to transmit commands coded in synthetic echo sequences, which, when received by the target radar, will be stored in system memory as if they were actual echoes from the monitored environment. Of course, this process - for now characterized only as EAM - by itself is not capable of altering normal radar operation. If the system is not compromised by a malicious computational process, this false information (entered via synthetic echoes) will be treated by the system and the operator as target or clutter data (BOLE; DINELEY; WALL, 2005). Although this EAM may disrupt the interpretation of what is happening in the environment, or even influence the user's decision making, the system will continue to operate as designed. However, if the system is compromised by a malicious computational process, it is possible to make the information inserted into the radar memory by synthetic echoes (transmitted by the attacker) be interpreted as commands. In this case, the cyber component of the cyber-electronic attack interprets the commands and can thus trigger malicious routines that alter the normal computational process of the system. These malicious routines may, for example, cause a system shutdown, interrupt the update of images to the operator, or even play previously recorded images of a normal operation - as supposedly occurred in the case of Operation Orchard (CLARKE; KNAKE, 2010).

As in the example above, other systems that process information received via the electromagnetic spectrum are also subject to cyber-electronic attacks. Without aiming to present a comprehensive list of potential targets for this type of attack, here are some examples:

- Radar and Automatic Radar Plotting Aids (ARPA) systems that generally make use of digitized video signals (BOLE; DINELEY; WALL, 2005). This includes, for example, navigational, air search and combination search radars used by civil and military vessels and facilities;

- Electronic Chart Display and Information Systems (ECDIS) (WARD; ROBERTS; FURNESS, 2000) that integrate into electronic charts information obtained from other systems such as radar, GPS, etc.;

- Integrated Bridge System (IBS), which interconnect radar/ARPA, GPS and other systems with Electronic Chart Display and Information Systems (ECDIS), as well as with ships' rudder control and propulsion systems (BHATTI; HUMPHREYS, 2017);

- Electronic Warfare Support Measurement Systems (ESM), typically composed of antennas, microwave receivers and computer systems responsible for processing, classifying and identifying the electromagnetic emissions present in the environment (MATUSZEWSKI, 2008).

These systems are usually kept isolated from other communication networks (and from the Internet). This means that in most cases the cyber component of the cyber-electronic attack must be able to overcome the air gap to reach the target's computing environment. However, despite the difficulty imposed by the air gap, these systems cannot be considered fully cyber-safe. As reported in the case of cyber-kinetic attacks, malware may cross the air gap through removable media. In addition, a logic trigger can be deployed to the target during manufacture or commissioning.

MULTI-DOMAIN ATTACKS

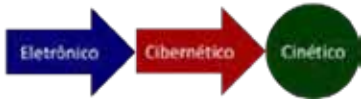
Our taxonomy defines multi-domain attacks as those whose execution exploits the three domains under discussion: cyber, electronic and kinetic. We have already conceptually discussed above how a cyber-electronic attack can manipulate a computer system - and trigger malicious processes - through synthetic commands/information received from the electronic warfare domain. Figure 2a presents and exemplifies this attack concept. We also conceptually discussed how malicious digital interferences in the cyber domain can produce direct kinetic effects on a physical plant through cyber-kinetic attacks. For comparison, we also present this attack concept in Figure 2b. In multi-domain attacks, the cyber component of the attack acts as a pivot between the electronic and kinetic warfare domains. As illustrated in Figure 2c, the cyber component can be

deployed to allow, for example, commands originating in the electronic warfare domain to be interpreted and converted into direct kinetic effects on a physical plant.

Figure 2 - Attack flows

a) Cyber-eletronic

b) Cyber-kinetic



c) Multi-domain

Therefore, the potential targets for this type of attack are systems that integrate electromagnetic wave transmission/reception equipment with computer systems that control physical plants. An example of a potential target for multi-domain attacks is the Integrated Bridge System (IBS), or Smartship systems (FULLERTON et al., 2004). Among the electromagnetic wave transmission/reception devices connected to an IBS are radar/ARPA systems, GPS receivers and AIS (Automatic Identification System) receivers. Typically, IBSs collect information from these systems in one place, plotting on a digital nautical chart information about the ship and other vessels - detected by navigation radars. The interconnection of the IBS with propulsion and rudder control systems enables the ship to function on autopilot, eliminating the need for continuous helmsman steering (FULLERTON et al., 2004; BHATTI; HUMPHREYS, 2017). The use of IBSs in naval vessels has the advantages of reducing crew size, increasing ship readiness, reducing training time, increasing situational awareness and reducing the administrative burden on personnel (FULLERTON et

al., 2004). These benefits have led to an increasing use of these systems on both merchant ships and warships (FULLERTON et al., 2004).

While IBS-type systems have several advantages, they can also expose naval vessels to new threats, such as multi-domain attacks. Just as the cyber component of a cyber-electronic attack can trigger malicious computational processes through the interpretation of commands received from the electromagnetic spectrum, so can a multi-domain attack. However, in a multi-domain attack, the malicious computational process, when triggered, extends its actions and reaches the computer-controlled physical processes. In an IBS, for example, this means that propulsion control may be affected by commands received by an antenna (e.g. a radar antenna) if the system is infected with malicious code capable of interpreting/converting the information received into commands to the ship systems.

Note that even if the target is protected by air gap, the cyber component of the attack could be inserted into the system through removable media. Moreover, as discussed above, this type of logic trigger can also be deployed into the target during manufacture or commissioning. This kind of attack is motivated by the attacker's ability to remotely trigger malicious routines that physically affect vessel functioning without the need for direct access to the target's cyber environment.

ATTACK MITIGATION POLICIES

In this section, we discuss some policies for increasing Sea Power security against these three attack classes. Considering that the cyber domain is common to all of these attacks, we focus on security-oriented policies for this domain. More specifically, we address policies on personnel qualification and product homologation and certification.

PERSONNEL QUALIFICATION

In 2003, the US government published its National Cyberspace Security Strategy (WHITE HOUSE, 2003), which states as its purpose:

> *"... to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact."* (WHITE HOUSE, 2003, p.VII)

While setting this objective, the document recognizes that:

> *"Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people."* (WHITE HOUSE, 2003, p.VII)

Indeed, protecting cyberspace is a complex strategic challenge. In this case, the first issue is to engage and empower the American people to secure the portions of cyberspace they use. This goal is difficult to achieve in full considering all of the society's elements and sectors mentioned in the Strategy (WHITE HOUSE, 2003). However, despite the difficulties imposed by its broad scope, there is an indisputable need for all nations to pursue the goal of involving and empowering its society in the security of the cyber environment.

Inspired by the US Strategy stated purpose (WHITE HOUSE, 2003), we also consider crucial to engage and empower Sea Power personnel to secure their portions of cyberspace. Although Sea Power represents a smaller public than the one targeted by the US Strategy (WHITE HOUSE, 2003), it is still a wide audience. For this reason, qualifying Sea Power personnel to secure their cyberspace portions is a challenging task, suggesting the need for personnel awareness and empowerment policies. These policies should cover not only Naval Power and Merchant Marine human resources, but also Sea Power industrial sectors and infrastructure.

In Brazil, the human resources of the Naval Power and the Merchant Marine are trained by the Naval Education System and the Maritime Professional Education System, both under the responsibility of the Brazilian Navy (BRAZIL, 2006). The curricula of these Education Systems should thus include subjects covering the functioning and security of the cyber domain and hybrid systems (in which the cyber domain interacts directly with the electronic and/or kinetic domains).

As discussed by Schneider (2013) and Conklin, Cline and Roosa (2014) – who address cyber security education targeting a wider audience than in the case of Navy and Merchant Marine - the biggest challenge is to promote the qualification of Sea Power personnel in its industrial and infrastructure sectors regarding cyber security and hybrid systems. This is because the vocational-technical training of its staff is provided by

many public and private institutions. Thus, based on Schneider (2013), it seems reasonable to conclude that it is not trivial to resolve the issue just by broad curriculum overhaul – even if it is necessary. In this case, it seems appropriate to first support these sectors through training and awareness programs promoted by the state agencies responsible for cyber security and defense in Brazil - i.e. the Institutional Security Office and the Army Command, respectively.

The US Department of Homeland Security, for example, does this by providing training programs offered by the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT). ICS-CERT continually offers cyber security courses for industrial control systems aimed at industry and critical infrastructure personnel in the US, as well as at equipment and software developers and suppliers. Importantly, ICS-CERT training programs are not restricted to the US Sea Power industry, but also cover other industry sectors. In the ICS-CERT model, this federal agency centrally supports the qualification of industry personnel in the subject. In the case of Brazilian Sea Power, taking into account the differences in scale, a similar model of centralized training support seems to be adequate to meet the needs of its industry and infrastructures regarding the safety of the systems discussed in this paper.

PRODUCT ACCREDITATION AND CERTIFICATION

We discussed above the possibility of a personnel-training strategy to promote the security of Sea Power cyber and hybrid systems. However, even though this kind of training is of utmost importance, it is not in itself sufficient to maximize system security (BAARS et al.; 2015). For greater security, personnel qualification policies should be complemented by policies on potential technological vulnerabilities in hardware and software.

System vulnerabilities may arise unintentionally (DU; MATHUR, 1998; GROVER; CUMMINGS; JANICKI, 2016), due to design, implementation or configuration flaws, or may be intentionally introduced by malicious agents (ADEE, 2008; ROBERTSON ; RILEY, 2018) during system design, manufacture, distribution, commissioning, operation or maintenance. One way to combat vulnerabilities - intentional or unintentional - is by adopting a set of security requirements, established according to the criticality of the system, which must be strictly met (HERRMANN, 2002).

The question then arises: How can we ensure that Sea Power equipment meets a set of specific security requirements, allowing the prevention or mitigation of a set of specific cyber security risks? This question raises a series of issues, which we will discuss below.

Consider the complexity of the production chain of hardware and software products used by the Navy, the Merchant Marine and Sea Power industries and infrastructures. The industry responsible for producing civilian, military or dual equipment for Brazilian Sea Power not only is not under the supervision of Brazilian cyber security and defense agencies, but also is part of the global electronic value chain, often relying on intricate production chains relying on outsourcing to foreign-based companies (PINTO, 2016) - making production monitoring even more difficult. Thus, even a full understanding of the cyber security requirements to be met by hardware and software does not ensure full confidence in an evaluation process based solely on "functional" testing - i.e. tests that assess the hardware or software behavior under typical operating conditions. In fact, according to the examples presented by Zetter (2014), Adee (2008) and Clarke and Knake (2010), if a device were to be interfered with by a hostile nation to cause malicious behavior, surely this would involve nontrivial operations, difficult to identify through testing merely based on typical equipment usage conditions.

Note that the literature has reported cases presenting evidence of malicious deployments on critical cyber systems, although there is often a lack of details due to confidentiality. An example is the attack on the Syrian air surveillance system occurred during Operation Orchard, which we already discussed above. As reported by Adee (2008), it was speculated that commercial Syrian radar microprocessors might have been purposely manufactured with a hidden backdoor. By sending a preprogrammed code to these chips, an unknown attacker could temporarily block the radar. On the deployment of vulnerabilities in hardware, Adee further states that:

> *"According to a U.S. defense contractor who spoke on condition of anonymity, a "European chip maker" recently built into its microprocessors a kill switch that could be accessed remotely.* (ADEE, 2008, p.1)

A more recent example of the deployment of malicious chips in critical system hardware is reported by Robertson and Riley (2018).

They describe a supply chain attack reported by Amazon.com Inc. to US authorities. In this case, experts have identified a tiny microchip, "not much bigger than a grain of rice" (ROBERTSON; RILEY, 2018), hidden in motherboards on servers. These microchips were not part of the original design of the boards. According to Robertson and Riley, investigators concluded that these chips allow attackers to create a stealth entry on any network using these altered motherboards. Moreover, researchers report that the chips were inserted in factories controlled by subcontractors in China (ROBERTSON; RILEY, 2018). Critical systems compromised by this supply chain attack include US Department of Defense data centers, CIA drone operating systems and networks aboard US Navy warships (ROBERTSON; RILEY, 2018).

Thus, in order to map and mitigate the risks associated with the use of software and hardware produced in unmonitored environments, some nations around the world have implemented accreditation systems for cyber products (FNCA, 2018; DSD, 2015; NIST, 2011; DISA, 2017). These methodologies allow the certification – with a minimum of confidence and through systematic testing and essays – that a software or hardware product meets a set of security requirements - even if the production process is not completely under the control and supervision of a country's security and cyber defense agencies. Examples of this kind of systems around the world are the Certification de Sécurité de Premier Niveau (CSPN) (FNCA, 2018) used in France, the Australasian Information Security Evaluation Program (AISEP) (DSD, 2015) implemented in Australia and New Zealand (DSD, 2015), the US Department of Defense Information Network Approved Products List (DoDIN/APL) and the Federal Information Processing Standard 140-2 (FIPS 140-2) (NIST, 2011) adopted in both the US and Canada.

Brazil has been occupying a relatively pioneering position in this area by establishing the so-called System of Homologation and Certification of Cyber Defense Products (SHCDCiber). SHCDCiber was designed in 2015 and aims to establish an objective cybersecurity assessment system based on leading international standards, ensuring scientific rigor in security assessments and international recognition by manufacturers who submit their products for evaluation.

Like the CSPN, AISEP, DoDIN/APL and FIPS 140-2 systems, SHCDCiber is designed to use compliance assessment mechanisms to evaluate the security of technological assets and equipment with

embedded software. It is thus a system with the potential to increase the security of Sea Power cyber and hybrid systems. SHCDCiber follows a three-step conformity assessment approach:

- Application risk analysis. Each application has a set of specific associated risks that should be considered in the design of evaluation mechanisms.

– Requirement specification. The exact safety requirements to be met by an application should be determined by the risks associated with that application.

- Safety tests. Compliance with a set of security requirements is achieved by performing tests following systematic validation procedures.

The three steps above, taken together, constitute a Conformity Assessment Program. With regard to information security, such programs are particularly challenging, since the behavior of an Information and Communication Technology (ICT) asset depends on its embedded software. Thus, studies are being conducted to increase confidence in security assessments of encryption (MACHADO et al., 2016; KOWADA; MACHADO; 2017), randomness (RIBEIRO et al. 2018), security protocols (MACHADO et al., 2015), software analysis (BENTO, 2017, forthcoming) and black box testing (TELES; MACHADO, 2017).

It should be noted that passing a compliance assessment program does not mean full confidence in the safety of the approved item. After all, requirements are specified according to application risks - and variations in the risk scenario may alter the security level of a product or system.

Critical analysis. Even after success in previous stages, depending on the item's criticality, the evaluation of additional aspects may still indicate that a technology should not be adopted. These aspects typically involve characteristics of the developer and of the production process. As an example, we have listed a few questions to be answered before adopting a technology - even if it has succeeded in steps 1 through 3:

- Is the technology supplier able to fulfill orders on the demanded scale?

- Does the technology provider have a system for information security management in place?

- More specifically in Sea Power systems, and depending on the criticality of the system, do developers and manufacturers - persons employed by public or private entities - have the appropriate security credentials to handle the product or technology in question?

- Does the technology provider comply with appropriate sensitive data protection and disposal procedures?

- Does the technology provider maintain its core production activities (production critical knowledge) in the country?

CONCLUSIONS

In this paper, we discussed how the encounter of cyberwarfare with electronic and kinetic warfare could have a direct impact on Sea Power. In order to address the new forms of cyberwarfare resulting from this meeting, we presented a taxonomy of hybrid attacks that, besides exploring the cyber domain, also explore the electronic and kinetic domains. Three classes of attack are thus defined — cyber-kinetic, cyber-electronic and multi-domain —broadening the range of application of the principle of kinetic effects. We discuss these three classes of attack and characterize, providing examples, their potential Sea Power targets. Our analysis, based on known cases, evidence and technological deductions, indicate a real possibility of these types of attacks affecting Sea Power. Thus, our study points to the need to develop policies capable of promoting the security of Sea Power cyber and hybrid systems.

Considering that the exploit of the cyber domain is common to the three attack classes analyzed in this article, we focused our discussion on security policies for this domain, addressing both personnel training and cyber products' vulnerabilities. Regarding personnel training, we encourage the adoption of a model supported by the existing systems of naval education and maritime vocational training, complemented by a centralized cyber security training body. The Naval Education System and the Maritime Vocational Training System, with continually updated curricula on the subject, would be in charge of training Naval Power and Merchant Marine personnel, respectively (as already currently happens). A centralized cyber security training body would be responsible for promoting the qualification of human resources in Sea Power industrial and infrastructure sectors. Regarding the mitigation of vulnerabilities in Sea Power cyber products, our study points to the adoption of a product accreditation and certification system, which is already adopted by countries such as France, Australia, New Zealand, USA and Canada. It is noteworthy that the policies on personnel training and on product accreditation and certification discussed here are not intended to fully

assure the security of Sea Power cyber and hybrid systems. However, they have the potential to contribute positively and extensively to the safety of these systems.

O ENCONTRO DA GUERRA CIBERNÉTICA COM AS GUERRAS ELETRÔNICA E CINÉTICA NO ÂMBITO DO PODER MARÍTIMO

RESUMO

A busca por melhores capacidades operacionais e gerenciais no Poder Marítimo tem motivado o aumento do uso de sistemas híbridos, em que componentes cibernéticos interagem com plantas físicas e com sensores/dispositivos que exploram o espectro eletromagnético. Entretanto, ao mesmo tempo em que esta integração traz vantagens, ela também expõe tais sistemas a novas ameaças, resultantes do encontro da guerra cibernética com as guerras eletrônica e cinética. O presente artigo analisa como estas novas ameaças podem afetar o Poder Marítimo, caracterizando, por meio de exemplos, seus possíveis alvos. Para dar suporte a esta discussão, propõe-se uma taxonomia que abarca novas classes de ataque que exploram os domínios cibernético, eletrônico e cinético. A análise aponta para a necessidade de políticas capazes de promover a segurança dos sistemas cibernéticos do Poder Marítimo. Neste viés, são discutidas políticas de qualificação de pessoal e de homologação e certificação de produtos cibernéticos, ambas com o potencial de contribuir de forma abrangente para a segurança do Poder Marítimo.

Palavras-chave: Guerra Cibernética. Guerra Eletrônica. Guerra Cinética. Poder Marítimo.

REFERENCES

AADEE, Sally. The hunt for the kill switch. IEEE Spectrum, v. 45, n. 5, p. 34-39, 2008.

AMIN, Saurabh et al. Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks. IEEE Transactions on Control Systems Technology, v. 21, n. 5, p. 1963-1970, 2013.

AMIN, Saurabh et al. Stealthy deception attacks on water SCADA systems. In: Proceedings of the 13th ACM international conference on Hybrid systems: computation and control. ACM, 2010. p. 161-170.

ARAKAKI, Glenn T. Yokosuka Naval Base Prepares for Nuclear Aircraft Carrier. Army Engineer School Fort Leonard Wood MO, 2009.

AYALA, Luis. Prevent Hackers from Destroying a Backup Generator. In: Cyber-Physical Attack Recovery Procedures. Apress, Berkeley, CA, 2016. p. 41-42.

BENTO, Lucila MS et al. Dijkstra graphs. Discrete Applied Mathematics, 2017. No prelo.

BHATTI, Jahshan; HUMPHREYS, Todd E. Hostile control of ships via false GPS signals: Demonstration and detection. NAVIGATION: Journal of the Institute of Navigation, v. 64, n. 1, p. 51-66, 2017.

BOLE, Alan G.; DINELEY, William O.; WALL, Alan. Radar and ARPA manual. 2. ed. Oxford: Elsevier Butterworth Heinemann, 2005.

BONNER, Henry M. The radio proximity fuse. Electrical Engineering, v. 66, n. 9, p. 888-893, 1947.

BOYES, Hugh; ISBELL, Roy. Code of Practice: Cyber Security for Ships. 2017.

BRASIL. Lei nº 11.279, de 9 de fevereiro de 2006. Dispõe sobre o ensino na Marinha. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato20042006/2006/Lei/L11 279.htm>. Acesso em: 29 out. 2018.

BROWN, Louis. The proximity fuze. IEEE Aerospace and Electronic Systems Magazine, v. 8, n. 7, p. 3-10, 1993.

CLARKE, Richard A.; KNAKE, Robert K. Cyber War: The next threat to national security and what to do about it. New York: Ecco, 2010.

DE SÁ, Alan Oliveira; DA COSTA CARMO, Luiz F. Rust; MACHADO, Raphael CS. Covert attacks in cyber-physical control systems. IEEE Transactions on Industrial Informatics, v. 13, n. 4, p. 1641-1651, 2017.

DIPERT, Randall R. Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. Journal of Military Ethics, v. 12, n. 1, p. 34-53, 2013.

DISA. Department of Defense Information Network (DoDIN) Approved Products List (APL) Process Guide. Defense Information Systems Agency (DISA). 2017. Disponível em: <https://aplits.disa.mil/docs/aplprocessguide. pdf> Acesso em: 28 out. 2018.

DSD. Australian government information and communications technology security manual. Defence Signals Directorate (DSD) Auditing, v. 3, p. 31, 2005.

ERICKSON, Kelvin T. et al. Reliability of S CADA Systems in Offshore Oil and Gas Platforms. In: Stability and Control of Dynamical Systems with Applications. Birkhäuser, Boston, MA, 2003. p. 395-404.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32. stuxnet dossier. White paper, Symantec Corp., Security Response, v. 5, n. 6, p. 29, 2011.

FLEMING, Paul et al. Field test of wake steering at an offshore wind farm. Wind Energy Science, v. 2, n. 1, p. 229-239, 2017.

FNCA. Catalogue of the Qualified Solutions. French National Cybersecurity Agency (FNCA). 2018. Disponível em: <https://www. ssi.gouv.fr/uploads/2018/01/catalogue_ qualified_solutions_anssi.pdf> Acesso em: 28 out. 2018.

FULLERTON, Jeff et al. Operational Impacts of the Aegis Cruiser Smartship System. NAVAL SEA SYSTEMS COMMAND WASHINGTON DC, 2004.

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, v. 29, n. 7, p. 1645-1660, 2013.

HART, Dennis. An approach to vulnerability assessment for Navy Supervisory Control and Data Acquisition (SCADA) system. 2004. Tese de Mestrado. Monterey, California. Naval Postgraduate School.

JANER, Denis; PROUM, Chauk-Mean. Open Architecture for Naval Combat Direction System. In: Complex Systems Design & Management. Springer, Cham, 2014. p. 73-84.

KAISER, Robert. The birth of cyberwar. Political Geography, v. 46, p. 1120, 2015.

KOWADA, L. ; MACHADO, R.C.S. . Esquema de Acordo de Chaves de Conferência Baseado em um Problema de Funções Quadráticas de Duas Variáveis. Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2017, Brasília, 2017.

KUMAR, Nishant; MAJUMDAR, Sayan; BABU, G. Madhu. Automatic control of tidal power plant. In: Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM), 2012 International Conference on. IEEE, 2012. p. 24-28.

LAGOUVARDOU, Sotiria. Maritime Cyber Security: concepts, problems and models. 2018.

LANGNER, Ralph. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, v. 9, n. 3, p. 49-51, 2011.

LASI, Heiner et al. Industry 4.0. Business & Information Systems Engineering, v. 6, n. 4, p. 239-242, 2014.

LEE, Jay; BAGHERI, Behrad; KAO, Hung-An. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, v. 3, p. 18-23, 2015.

LUNA, D. Petrobrás vai gerar energia eólica no mar. O Estado de S.Paulo, São Paulo, 24 de julho de 2018. Disponível em: < https://economia. estadao.com.br/noticias/geral,petrobras-vai-gerar-energia-eolica--nomar,70002412545> Acesso em: 17 out. 2018.

MACHADO, Raphael CS et al. Fair fingerprinting protocol for attesting software misuses. In: Availability, Reliability and Security (ARES), 2015 10th International Conference on. IEEE, 2015. p. 110-119.

MACHADO, Raphael CS et al. Software control and intellectual property protection in cyber-physical systems. EURASIP Journal on Information Security, v. 2016, n. 1, p. 8, 2016.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. Livro verde: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

MARINHA DO BRASIL. Doutrina Básica da Marinha. Rev. 2. Brasília 2014.

MATUSZEWSKI, Jan. Specific emitter identification. In: Radar Symposium, 2008 International. IEEE, 2008. p. 1-4.

MILLER, Bill; ROWE, Dale. A survey SCADA of and critical infrastructure incidents. In: Proceedings of the 1st Annual conference on Research in information technology. ACM, p. 51-56, 2012.

MINISTÉRIO DA DEFESA. Política de Guerra Eletrônica de Defesa – MD32-P-01, 1ª Edição, 2004.

MINISTÉRIO DA DEFESA. Manual de Doutrina Militar de Defesa – MD51-M-04, 2ª Edição, 2007.

MINISTRY OF DEFENSE. UK Defense Doctrine – Joint Doctrine Publication 0-01. 5 ª Edição, 2014.

NIST. FIPS 140-2: Security Requirements for Cryptographic Modules. National Institute of Standards and Technology (NIST) v. 25, 2001.

NORCUTT, L.S. Ship Self-Defense System Architecture. Johns Hopkins Apl Technical Digest, v.22, n.4, p. 536-546, 2001.

ORTIZ, G. P.; KAMPEL, M. Potencial de energia eólica offshore na margem do Brasil. Instituto Nacional de Pesquisas Espaciais. V simpósio Brasileiro de Oceanografia, Santos, 2011.

PARKS, Raymond C.; DUGGAN, David P. Principles of cyberwarfare. IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.

REED, Thomas C. At the abyss: an insider's history of the Cold War. Presidio Press, 2005.

RIBEIRO, Leonardo C. et al. True Random Number Generators for Batch Control Sampling in Smart Factories. In: 2018 Workshop on Metrology for Industry 4.0 and IoT. IEEE, 2018. p. 213-217.

ROBERTSON, Jordan.; RILEY, Michael. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg Businessweek, 04 de

outubro de 2018. Disponível em: <https://www.bloomberg.com/ news/ features/2018-10-04/the-big-hack-how-china-used-a-tiny -chip-toinfiltrate--america-s-top-companies> Acesso em: 27 out. 2018.

SHAKARIAN, Paulo. The 2008 Russian cyber campaign against Georgia. Military review, v. 91, n. 6, p. 63, 2011.

SHELTON, H. JP3-13: Joint Doctrine for Information Operations. 1998. http://www.c4i.org/jp3_13.pdf.

SMITH, Roy S. Covert misappropriation of networked control systems: Presenting a feedback structure. IEEE Control Systems, v. 35, n. 1, p. 82-92, 2015.

STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, v. 800, n. 82, p. 16-16, 2011.

SUN, Xiaojing; HUANG, Diangui; WU, Guoqing. The current state of offshore wind energy technology development. Energy, v. 41, n. 1, p. 298312, 2012.

TELES, C. ; MACHADO, R.C.S. . Testes de sobrecarga: uma avaliação sobre requisitos de Disponibilidade e Desempenho. Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Workshop sobre Regulação, Avaliação da Conformidade, Testes e Padrões de Segurança (SBSeg/WRAC+), Brasília, 2017.

TOPALOV, Andriy; KOZLOV, Oleksiy; KONDRATENKO, Yuriy. Control processes of floating docks based on SCADA systems with wireless data transmission. In: Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2016 XII International Conference on. IEEE, 2016. p. 57-61.

WADHAWAN, Yatin; NEUMAN, Clifford. Evaluating Resilience of Oil and Gas Cyber Physical Systems: A Roadmap. In: Annual Computer Security Application Conference (ACSAC) Industrial Control System Security (ICSS) Workshop. 2015.

WARD, Robert; ROBERTS, Chris; FURNESS, Ronald. Electronic chart display and information systems (ECDIS): State-of-the-art in nautical charting. Marine and Coastal Geographical Information Systems, p. 149161, 2000.

WEIGLEY, Russell F. JP1 Doctrine for the Armed Forces of the United States. 2013.

WEISS, Gus W. The Farewell Dossier. Center for the Study of Intelligence, Central Intelligence Agency (CIA), Washington DC, 1996.

WHITE HOUSE. The national strategy to secure cyberspace. Washington, DC: White House, 2003.

YASAR, Nurgul; YASAR, Fatih Mustafa; TOPCU, Yucel. Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield. In: Cyber Sensing 2012. International Society for Optics and Photonics, 2012.

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books, 2014.

ZIVI, Edwin. Design of robust shipboard power automation systems. Annual Reviews in Control, v. 29, n. 2, p. 261-272, 2005.