CYBERSPACE: THE CHALLENGES OF NORM FORMATION[1]

O CIBERESPAÇO: OS DESAFIOS DA FORMAÇÃO DE NORMAS

DOI: 10.5380/cg.v10i1.78424

Maria Claudia Menezes Leal Nunes[2]

Abstract

The rules of appropriate conduct in cyberspace have always been a discussion throughout the various years, especially between States. With the rapid expansion of cyberspace, the creation of an international regime for the conduct of States became necessary, however, the many different vulnerabilities, actors, and even definitions made the consensus process difficult. The attributional question of cyberspace, however, was the question that most impeded the process. Technical advances in this area, along with the use of legal standards of proof made public attribution possible and more common. This paper seeks to investigate the link between public attribution with what is possibly an embryo of an international regime for cyberspace with a case study of NotPetya as emblematic of this trend.

Keywords: Cyberspace; Public Attribution; International Regimes.

Resumo

As regras de conduta apropriadas no ciberespaço sempre foram uma grande discussão ao longo dos anos, especialmente entre os Estados. A rápida expansão do ciberespaço tornou necessária a criação de um regime internacional para a conduta dos Estados, no entanto, as diversas vulnerabilidades existentes, atores e até definições diferentes dificultam o processo de consenso. A questão de atribuição de cyber incidentes, no entanto, era a questão que mais impedia o processo. Com avanços técnicos nesta área juntamente com a utilização de processos investigativos legais, atribuição pública está se tornando mais comum. Este estudo investiga a ligação entre atribuição pública e o que é possivelmente um novo regime no ciberespaço, utilizando um breve estudo de caso do NotPetya e como este é emblemático desta nova tendência.

Palavras-Chave: Ciberespaço; Atribuição Pública; Regimes Internacionais.

1. INTRODUCTION

The natural progression of technology created an expansive and new area of research for the field of International Relations. Already in the 20th century, two new technologies came into existence that created large ripples in the study of security in the field, space, and nuclear technology.

[1] Este artigo está licenciado sob a Licença Creative Commons Attribution (CC BY 4.0), sendo permitido o compartilhamento com reconhecimento da autoria e publicação inicial nesta revista.

[2] Mestranda do Instituto de Relações Internacionais da Universidade de São Paulo (USP). E-mail: mariaclmnunes@gmail.com. ORCID: https://orcid.org/0000-0002-6892-1186.

The first lead to an explosion of debates over military and legal implications of the technology, while the second led to one of the most famous theories from Kenneth Waltz, that the greater diffusion of nuclear technology would mean greater safety (Sagan and Waltz, 1981). Now in the widespread implementation of the Internet of Things and on the cusp of the Fourth Industrial Revolution, security discussions regarding new technologies are needed along with new international norms over said technologies.

With its commercialization, cyberspace has undergone a large expansion and refinement of its interconnectivity through the generations, leading to a natural evolution of security studies pertaining to it. The evolution of security studies would occur with a technological milestone or an international event in cyberspace, for example, the US Election Interference in 2016, would shift focus within the security studies field. As part of this evolution, two distinct areas of studies have been identified that may cause great ambiguity in the field of security studies and policies that are applied to such a nascent, but domineering field. While both areas are described as cybersecurity politics, the different emphasis on the title will lead to disparate studies on the subject; one focusing on politics in cybersecurity and the other focusing on cybersecurity in politics (Cavelty and Wenger, 2020). It is from this ambiguity that this paper aims to contribute to the study of security norms in cyberspace, and their creation.

The necessity of governing norms in cyberspace has come from how these political influences are being utilized in cyberspace, along with small-scaled, but constant cases of cyberattacks. Yet, there is not a universal convention of social conduct norm in which all countries follow (Change and Grabosky, 2017), nor a framework which States can utilize as a precedent to react to cases of cyberattack and exertion of influence through cyberspace. The creation of such response framework and norm for social conduct becomes even more muddled and confusing when in research it has been acknowledged that States are not the only actors that influence the domain (Singer and Friedman, 2013; Change and Grabosky, 2017). This in turn has created various new dynamics that are prevalent in cyberspace, a melding of private companies, international organizations, and individual groups that meld together to create a kaleidoscope of dynamism that require negotiation amidst themselves and states for a system that, while resembles governance, does not set social conduct norms nor does it punish deviate behaviors online.

This paper focuses on the governance of cyberspace and how attribution can be utilized as a method of setting social norms of acceptance of interstate behavior in cyberspace utilizing a previously established framework with few modifications to punish actions that certain destructive behaviors that State may engage in or not prevent. With public attribution becoming commonplace, the possibility of cyberspace norms being finally created becomes clearer.

The current working paper is divided into four sections. The first one takes a brief look at the current problems in cyberspace governance that impede a norm. It problematizes the concept of cyberspace and how the construction of the domain creates hurdles in the creation of norms of conduct within cyberspace. The second section looks at the securitization of the cyberspace domain. Utilizing the critical lens provided by Lobato and Kenkel (2015), the paper applies the logic of the Copenhagen school which places cyberspace as its own referent object, which actors securitize. The third section analyzes the effectiveness of proposed frameworks to deal with cyberattacks that operate within cyberspace and the possible responses that States may have. The final section discusses the case of NotPetya, contrasting them with the evidence from Crain and Nadler (2019) where the internet advertising infrastructure can be used as a tool for power plays.

2. THE GOVERNANCE OF CYBERSPACE

The existence of cyberspace as a domain that transcends physical borders, occupying both a tangible and intangible existence. Peculiarities of its existence tend to create hurdles for a governance system to be created for the domain, in other words, a singular institution that can implement social conduct laws within this domain. Among these peculiarities, we find the architecture of cyberspace, actors, and the definitions therein to be the most problematic in the case of norm creation and application.

Fundamentally, cyberspace is understood to be an artificial domain created by humans, which occupies an existence that sits on deterritoriality and territoriality. As explained in Medeiros and Goldoni (2020), the nature of cyberspace does more than cross borders, but also anchors such to a physical territory through the equipment used to access the infoways. It is a full domain that encompasses the traditional domains, penetrating them through interconnected informational flows, and challenging the zonal conception of territory. This challenge doesn't go unnoticed and actually brings a host of problems in terms of jurisdiction. The interconnection makes it hard to enforce laws over certain activities that, while may be legal in certain states, are illegal in others (Singer and Friedman, 2014), as well as the applicability of copyright laws that may not be exercised depending on the physical location of the servers of where the content is hosted[3]. Henceforth, there have been several attempts at harmonizing criminal and procedural national cyberspace laws, none have ever definitely solved this territorial conundrum.

There have been two attempts notable multilateral attempts to solve this issue of territoriality, the first one being the Convention of Budapest of 2004 while the second attempt has been the Tallin Manual of 2013. However, these two attempts have not been able to give closure to the issue of territoriality and have rather limited applicability. The Convention of Budapest failed on the principle that it has a very limited scope as it deals in principle only with the occurrence of

[3] One example would be the case of the application of Japan's Copyright Act of 1970 in videos on YouTube, in which the servers are in the United States. Due to the Digital Millennium Copyright Act of 1998, in which YouTube functions under the laws of Fair Use from the United States apply to media from Japan that are used in transformative works hosted in YouTube servers.

cybercrimes, notwithstanding, the small number of countries that ratified the convention along with missing key players such as China, India, and Brazil limit the applicability of the treatise cyberspace (Chang and Grabosky, 2017). As an attempt to harmonize the definition and criminal offense of cybercrimes there are a few factors that may have induced the failure of the convention overall. One of the main concerns is the general lack of a common definition that is agreed on by different countries. This can be verified when looking at the definition of cyberwarfare between, for example, the United States and Russia, in which for the former the definition of cyberwarfare characterizes it as "cyberattacks that are authorized by state actors against cybernetic infrastructure in conjunction to a government campaign" (Giles and Hagestad II, 2013, p. 4), while the latter defines cyberspace warfare as "cyberattacks done by States, groups of States, or politically organized groups against cyberspace infrastructure, all part of a military campaign" (Giles and Hagestad II, 2013, p. 4). Both definitions present similarities, however, the nuance between the difference of government campaign and military campaign, along with the definition that excludes military political organizations brings a problem with cyber incidents with the participation of non-state actors (Giles and Hagstad II, 2013).

A similar issue occurs when one would look at the second attempt at creating a codified norm through the Tallin Manual. Officially, it never presented itself as a document to act as a codifying law or a norm. Instead, it sought to present itself as a framework which states could utilize in order to deliberate over cybernetic incidents and decide if legal action is necessary and which legal action it would take. Unlike the Convention of Budapest, however, the scope of the Tallin Manual is much narrower, focusing on the incident that would be jus ad bellum and jus in bello principles (Schmidt, 2013). Activities that fall under the criminal umbrella are not dealt with in the Tallin Manual, instead, an almost exclusive focus is given to activities that deal kinetic damage, as pointed in Section 1, article 1, ¶ 6: "The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty" (Schmidt, 2013, p. 16).

Both the Convention and the Tallin Manual, while prolific attempt to establish international norms within cyberspace, they have not been able to accomplish much. Lack of a traditional zonal territoriality (Medeiros and Goldoni, 2020) tied together with the lack of a common vocabulary (Giles and Hagestad II, 2013) creates an environment where public attribution becomes a prime method, which create norms of conduct in cyberspace and, at the same time, can be debatable and contestable in the international arena (Egloff, 2020). In addition to these two points, there are structural factors that create suspicion within public attributions such as economic and political incentives from both State and non-State actors that further muddle the water of what is acceptable or not within cyberspace (Cavelty and Wenger, 2020; Egloff, 2020).

However, this does not mean that there are not any existing structures that constrain states or non-state actors within cyberspace. There is an order that exists within the domain. It is comprised of an amalgamation of decentralized informal institutions that fit together like a mosaic to regulate it along with State institutions, governments frame these informal institutions together. These governmental frameworks are then joined together as varying governing norms that are joined and fit together, but there is not a solid framework that ties all together neatly[4]. Nevertheless, without a global institution that a universal consensus and rules, attribution in cyberspace will inevitably have politically uncertain gains due to various intrinsic factors within the domain (Egloff, 2020). It is important then to understand the process of securitization how it forms the current cyberspace structure.

3. SECURITIZATION OF CYBERSPACE

Security threats, according to the Copenhagen School, are constructed through speech, where a certain object, called the referent object, is deemed to be above what is considered to be above normal politics (Buzan et. al., 1998). The theory as a post-structuralist theory in order to broaden the scope of what was considered to be a security threat and explain the various dynamics therein the various sectors it proposed. Later, the framework was expanded beyond the original sectors in order to capture the unique dynamics within cyberspace (Hansen and Nissebaum, 2009) and expanding the securitizing actors beyond the State, including actors such as think tanks, giving plausibility for private agents to become securitizing actors themselves (Lobato and Kenkel, 2015).

This paper argues, then, that the securitization of cyberspace has contributed to the creation of structures that are hurdles to the creation of global cyberspace norms, all the while, also creating a division between knowledgeable cyberspace professionals lined by good and bad science (Lobato and Kenkel, 2015; Tanczer, 2020).

Starting with the structure, it must be understood that the dynamics that are present in cyberspace are understood to be the result of the securitization of cyberspace. Precisely speaking, with networks themselves as the referent object, allows multiple actors to become both victims and perpetrators of the cyberattacks from a host of different types of attacks (Lobato and Kenkel, 2015).

The dynamics within cyberspace have been identified: Code Regulation, Self-Regulation, and Distributed Security. Each of these dynamics operates in a different manner that converges formal regulation as well as informal regulating bodies in differing proportionality. The first of these, and most formal of the three, code regulation, postulates that the very architecture of cyberspace space is formally regulated by governments thusly forcing technology companies to adequate themselves to formal rules in order to function (Chang and Grabosky, 2017). In this instance, governments

[4] There are bilateral and multilateral agreements that bind national state institutions together that lead to various governing norms to be stitched together. However, this does not mean there is one uniform norm that can be fully applied as there are more actors than states that act within cyberspace.

become the securitizing actor, thusly, applying certain rules as an effort to reduce the vulnerabilities by adjusting the very code foundation that cyberspace is inserted within. However, as an effect of this regulation, the issue of cyberspace freedom and anonymity comes into play (Chang and Grabosky, 2017), again, as a result of securitizing speech that has led, in some States, a creeping militarization of cyberspace such as the United States (Lobato and Kenkel, 2015) and China. Within the second dynamic cited, self-regulation has the market as an informal regulator, though governments may provide legitimacy to certain institutions to enforce mandates (Chang and Grabosky, 2017). It is within this dynamic that we find a greater amount of division within the professionals of cybersecurity between different categories, constructing almost an in-group and out-group perception of those that are hackers and employ such tactics in favor and against private entities. These perceptions on hackers and their identity also create a microcosm of what are acceptable practices and behaviors within the field (Tanczer, 2020), which can influence the self-regulation itself. The last of the dynamics explored is the distributed security, where the burden of security is distributed among various actors in the sphere, allowing for the sharing of information to bolster informational security, relying both on government, private sector, and active users as a source of policing (Chang and Grabosky, 2017). Proposals of a distributed security system dynamic build upon the notion that the entire network needs to be securitized (Lobato and Kenkel, 2015) by creating speeches over the need to impose certain habits upon users interconnected in cyberspace or software in order to increase security within the network and quarantine any cyberattack outbreak (Chang and Grabosky, 2017).

These dynamics are an effective way to look to cyberspace and the myriad of ways that security can be established. There is not one dynamic that predominates the cyberspace domain, however, the effects that these kinds of dynamics have are reflected in a structure that creates an arena in which public attribution, though technically feasible, is often contested (Egloff, 2020). Within the securitized domain of cyberspace, the threat of the exploitation of vulnerability (Lobato and Kenkel, 2015) creates a structure of incentives towards private companies (Chang and Grasbosky, 2017; Egloff, 2020) that muddles the water. As explained by Egloff (2020), private companies, especially cybersecurity companies, have economic and political incentives to provide, or withhold, information to governments that may utilize this information to create a public attribution claim. Some private companies may elect to keep breaches of security a secret in order to keep themselves from being punished by governments (Chang and Grasbosky, 2017) or from inspiring copycat incidents (Singer and Friedman, 2014; Egloff, 2020), yet other companies, particularly cybersecurity companies, may want to advertise their expertise by publishing technical information (Egloff, 2020). Political biases also fall in line with incentives that these companies may have as Western-based companies tend to not divulge information on Western activities (Egloff, 2020). Additionally, with the various existing actors in cyberspace that may perpetrate cyberattacks in the domain (Singer and Friedman, 2014; Egloff, 2020), securitization speech, that is embedded *within* public attribution, may serve as incentives for governments to covertly align themselves to traditionally marginalized hacking communities in order to deflect any blame that may arise from public attribution despite the fact that there are hackers that are in government or private company employ (Tanczer, 2020).

4. STRUCTURE OF ANALYSIS FOR THE ATTRIBUTION OF CYBER INCIDENTS

In regard to cyberspace itself, interconnectivity and its expansion did not encompass solely the informational sphere with information sharing being done promptly, as it has started to encompass other spheres of society such as the political and economic sphere (Cavelty and Wenger, 2020). Though this technological process has been beneficial to many states and their development, society has become vulnerable in these same areas. With critical infrastructure and the economy becoming more interconnected, the sharing of source codes between State and private companies make these same vulnerabilities more dangerous as time goes by. Since if a vulnerability is taken advantage of, the harm to a system network would be incredibly widespread (Chang and Grabosky, 2017; Stevens, 2012).

This spread of cyberspace into different spheres prompted States to look at cyberspace as a case of national security, with perhaps the most prominent of which is the United States. The study of such space has led to the attempted creation of a framework, though there are a few criticisms to utilizing a military mindset when engaging within the domain to create such a framework (Kallberg and Cook, 2017). Nevertheless, the discussion of a possible framework is important when it comes to setting the standard to how cyberincidents can be evaluated. Without a framework, case studies, such as NotPetya, Sony Entertainment, and the case of the 2016 Democratic Committee (Egloff, 2020), would seem to have been punctuated by irrational State behavior. Yet, coming from the principle that States are rational actors, one needs to have a framework in order to evaluate possible actions that States will take.

A principal question about the framework utilized would be regarding the translation of the traditional military tenets into the domain, which has been largely criticized for being largely outdated and woefully inefficient for the challenges that the domain holds (Kallberg and Cook, 2017). However, a framework has been developed that does employ a different methodological tool in order to deal with the unique challenges that comes from the domain, among which consist of subjective analysis that comes from legal processes (Mejia, 2014). Consisting of two vertices, the proposed analytical framework orients the incident on a scale of damage and perpetrator identification (Mejia, 2014), two tenets that have been criticized largely for a lack of effective measurement and anonymity (Kallberg and Cook, 2017).

The vertex that scales the severity of damage taken by a State measures the possibility of a retaliatory act against a possible perpetrator. Public norms regarding retaliation have been codified into international law with the statement that States may only use force in self-defense[5]. Criticism in regard to the severity of the attack often states the attackers do not know the scale of damage that an attack may have against an enemy network upon execution (Kallberg and Cook, 2017). There is a lag of time between the execution of a cyberattack and the investigation on the damages caused, creating difficulties in assessing what would be the proportionality of an attack. By the rules set forth by the Laws of Armed Conflict (LOAC)[6], a retaliatory attack is only permissible if it manages to cause the same damage that a victim State received (Mejia, 2014; Singer and Friedman, 2014). Factoring the interconnection between civilian, State, and military infrastructure, the permission of retaliation becomes a delicate legal question (Mejia, 2014; Singer and Friedman, 2014; Hieginbotham et. al. Chang and Grabosky, 2017) as spillover damage from cyberattack may escalate to kinetic attacks (Stevens, 2012; Mejia, 2014; Heginbotham et. al., 2015).

The legal question presented, however, is solved by the application of the Article 52 (2) of the Additional Protocol of the Geneva Convention[7] by a victim State, as it is stated within the article itself that if the targeted object constitutes itself as giving military advantage, it is then an object that can be legally destroyed, either partially or totally (Mejia, 2014). While there is a great systemic lag for the case of a retaliatory attack, as attacks are considered to be executed at a computational speed while defensive strategies take time to create and execute (Kallberg and Cook, 2017), it is not a defect, but rather a feature. The time that is necessary to create a strategy creates two advantages for a dynamic framework: a) it permits the deliberation of alternatives to a retaliatory strike, such as diplomatic pressure or strengthening of defensive systems or b) permits the victim State to retaliate in a limited manner that does not create spillovers.

The most emblematic case of the latter option is the case of Stuxnet. It was not a retaliatory strike, however, the development and specificity of the worm's coding permitted it to affect only one specific system without generating damage to other systems not specified in the code (Porche III, Sollinger, McKay, 2011). As a result of this very specific coding, if an infected system didn't have the target program specified in Stuxnet's code, the worm would become inert. Additionally, the worm had a code line of self-destruction that would become active after a certain date and after the limit number of infections was hit (Singer and Friedman, 2014). The success of the Stuxnet demonstrates that it is possible, with given time, to create a retaliatory cyberweapon that targets only military systems while leaving civilian networks relatively unscathed. Therefore, it is possible to follow the

[5] See: CHARTER of the United Nations. 1945. Available in: https://legal.un.org/repertory/art51.shtml .

[6] This law, also known as International Humanitarian Law (IHL), seeks to limit the effects of armed conflict due to humanitarian concerns.

[7] Article 52 (2) of the Additional Protocol of the Geneva Convention delimits military objectives as objects that their nature, objective, or use effectively contributes to military actions where a total or partial destruction, capture, or neutralization in the circumstances of the retaliation defines itself as a military advantage.

proportionality clause of the Law of Armed Conflict, however, it does call into question the costs and benefits of such actions like Stuxnet[8]. In this same vertex, the severity is examined in order to find if the LOAC is applicable to the situation, to which six criteria[9] exist: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. When these six criteria are applied to a cyber incident, it may help the Statist to determine if the incident is equivalent to a traditional kinetic attack and if a retaliation is both necessary and permissible through the LOAC (Mejia, 2014).

The second vertex of this analysis framework concerns actor attribution. One of the main issues of the domain, it is generally accepted as being extremely difficult for one State to make a public attribution as the participation in this domain is not restricted to States, but rather, non-state actors as well (Singer and Friedman, 2014). Tools also exist that can be employed to mask the network trail that can lead to the culprit. The typical method of tracking culprits, IP tracing, can be easily bypassed by the use of IP address spoofing (Mejia, 2014; Chang and Grabosky, 2017), which leads to the assumed difficulty in attribution (Singer and Friedman, 2014). However, the technical difficulty in full attribution to a State is mitigated by political-analytical frameworks that have been discussed by a few authors (Healy, 2013; Mejia, 2014; Cavelty et. al., 2015). However, by utilizing the subjective political-analytical nature of the cyber incidents, actor attribution can still be linked towards a state, whether or not the incidents were caused by agents of the State according to the framework.

A political-analytical framework regarding actor attribution remains one of the most important points of the process for the analysis of cyber incidents. A technical proof will never provide complete and irrefutable proof due to the asymmetrical information structure that exists (Egloff, 2020), henceforth requiring a more holistic approach that is provided by different fields such as the legal profession and law enforcement (Mejia, 2014). This falls in line with not exploring which specific actor caused the incident, but rather, which State is responsible for it (Healy, 2013; Mejia, 2014; Cavelty et. al., 2015). Within such framework, there are two types of attribution that exist: direct attribution[10] or indirect attribution[11], which is further reinforced when taking into account fourteen analytical points that reinforce the holistic nature of the legal standard practice.

The fourteen points are as follow: tracing to a nation, tracing to a state organization, attacks written or coordinated in national language, state control over the Internet, technical sophistication, little societal anger at target, no direct commercial benefit, direct state support of hackers, strong

[8] Although the costs and benefits of a cyberweapon does not factor into the scope of this paper, Max Smeets has written about this subject in a blog post in the Council of Foreign Relations (2016) and while not directly relating the costs of cyberweapon creation, C. Easttom (2018) explores the process of creation of such weapons though also relating that Stuxnet was technically an operational failure.

[9] These criteria are part of the Schmitt model, as proposed by Michael N. Schmitt professor of international law at the University of Reading.

[10] Direct attribution would be the States are responsible for actors or omission of individuals exercising the state's machinery of power and authority even if the acts exceed the authority granted by the (Mejia, 2014).

[11] Indirect attributions are acts or omissions of non-state actors that are attributable to the state if the state fails to exercise due diligence in preventing or reacting to such acts or omissions (Mejia, 2014).

correlation with statements from national leadership, lack of openness and cooperation, strong correlation with national policy, lack of any other nation or group that benefits or correlated or integrated with physical force (Healy, 2013). These points, coupled together with the legal practice of standards of proof, bypasses the need for irrefutable technical proof (Mejia, 2014) as due to the political structure and lack of international normative practices leads to cases where the technical proof might be contested, such with the case of Sony Entertainment Pictures in 2014, and the DNC in 2016 (Egloff, 2020). Henceforth, one does not seek to attribute the cyber incident to an actor, but instead seeks to attribute responsibility to a State, that falls in the spectrum going from direct aiding or gross negligence.

TABLE I – SPECTRUM OF STATE RESPONSIBILITY

Type of Stance	**Government Influence Level**
State-prohibited	The national government will help stop the third-party
State-prohibited-but-inadequate	The national government is cooperative but unable to stop the third-party attack
State-ignored	The national government knows about the third-party attacks but is unwilling to take any action
State-encouraged	Third parties' control and conduct the attack, but the national government encourages them as a matter of policy
State-shaped	Third parties control and conduct the attack, but the state provides some support
State-coordinated	The government coordinates third-party attackers, such as by "suggesting" operational details
State-ordered	The state directs third-party proxies to conduct the attack on is behalf
Rogue-state-conducted	Out-of-control elements of cyber forces of the state conduct the attack
State-executed	The state conducts the attack using cyber forces under their direct control
State-integrated	The state attacks using integrated third-party proxies and its own cyber forces

Source: HEALY (2013).

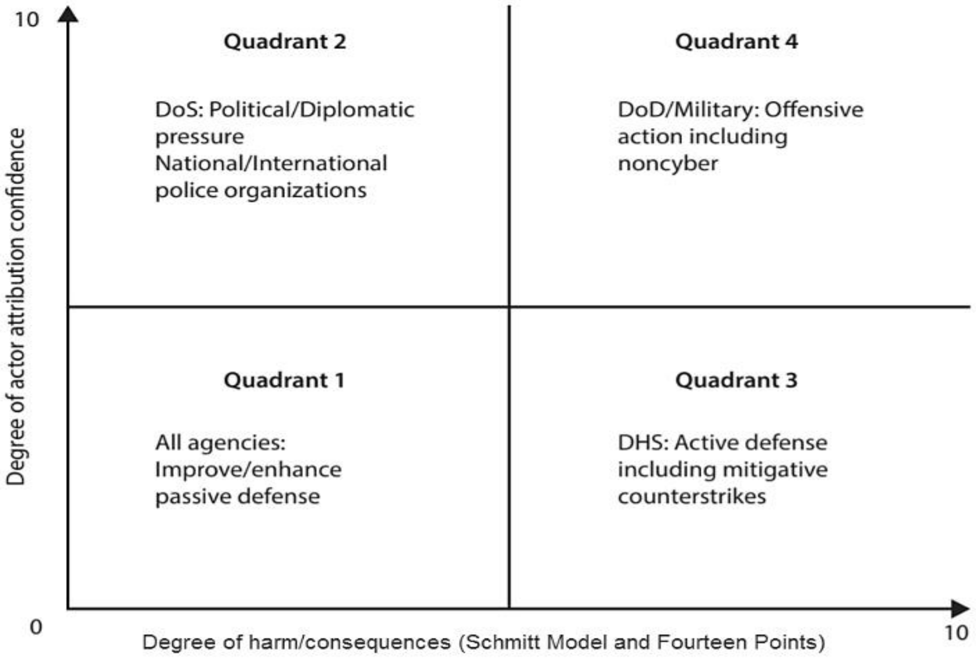
All of this comes together in the framework in order to create a solid analytical case-by-case study of cyber incidents and the most appropriate responses to them that States might have. In the framework, this is represented by the quadrants in which the vertices of Act Attribution and Actor Attribution intersect. While originally proposed by Colonel Mejia utilizing only the Schmitt Model in the Actor Attribution vertex, the author of this paper modifies the framework and adds the fourteen points as described by Healy as a complement for the vertex of Actor Attribution. The second figure illustrates the modified model, along with the suggested actions for each quadrant.

Even with this framework, there are aspects to it that will come under valid criticism due to the nature of cyber incidents. Unlike case studies, cyber incidents are dynamic, in other words, they do not remain static with one appropriate response. As the investigation of a cyber incident goes on and as more information is revealed, the appropriate response to a cyber incident might change

(Mejia, 2014). This may in part explain delays in responses of cyber incidents, that the more thorough the analysis of a case is the slower the response to the incident will be. In turn, this might damage the case of public attribution.

Another criticism that can be made of the framework model is how the responses are framed inside of the model. What is proposed of the model is to limit the severity of responses accordingly to the cyber incident, however, there might be less severe responses that are not listed in the framework that might be used. The framework is not a formula that will predict with full accuracy of how a State will act in response to a cyber incident as not necessarily a State will have to take one of the actions described in it (Mejia, 2014). The unique dynamics of cyberspace are captured by this very framework. As discussed in the third section of this paper, the securitization process of cyberspace, with networks as the referent objects, permits private actors, such as think tanks and individuals to be a victim as well as perpetrators of different types of attacks in this space (Lobato and Kenkel, 2015), however, States, have a privileged position in setting the security agenda overall due to being historically endowed for this purpose (Hansen and Nissenbaum, 2009). As a result of this privilege, it endows States with the possibility of utilizing public attribution as a form of securitizing speech, and it is this securitizing speech that inevitably underlies this framework that presents an ambiguity. It reinforces a structure that widens a gap of information asymmetry, yet at the same time, public attribution as a form of securitizing speech sets a precedent to what is considered acceptable or not acceptable in cyberspace. It is the framework of this section, with its underlying securitized understanding of cyberspace, that allows States to perform public attribution with incremental political gains that set the groundwork for a future cyberspace norm.

FIGURE I – MODIFIED ANALYTICAL MODEL FOR ATTRIBUTION


10
Quadrant 2
DoS: Political/Diplomatic pressure
National/International police organizations
Quadrant 4
DoD/Military: Offensive action including noncyber
Quadrant 1
All agencies: Improve/enhance passive defense
Quadrant 3
DHS: Active defense including mitigative counterstrikes
Degree of actor attribution confidence
0
Degree of harm/consequences (Schmitt Model and Fourteen Points)
10

Source: Mejia (2014).

5. ATTRIBUTION AND ITS NORMATIVE FUNCTION

Public attribution has become more common despite the lasting belief that technical difficulties make attribution an almost herculean and impossible task (Egloff, 2020). In some of the most notorious cases of public attribution, the international community as a whole has had different reactions, with some being contested[12], and others generating discourse[13] and others have had support when there was a public attribution[14]. The very technical impossibility of irrefutable certainty of attribution of cyber incidents (Mejia, 2014), creates the political structural factors that cause distortions of public perception. Notwithstanding the incentives extrapolated in previous sections of this paper of private companies hiding the existence of a cyber incident, security companies, while willing to release public information on cyber incidents, have their own set of incentives that distort the viewing of the cases of public attribution.

The first of these incentives are for security companies to not investigate all cyber incidents that occur. The reason is due not only political, as the governments often contract these companies to investigate cyber incidents, but also economical as cybersecurity companies will seek out only a limited number of cyber incidents to investigate in order to gain visibility and demonstrate their expertise (Egloff, 2020). The second incentives are the very asymmetric press released that contribute to the first incentive. The scope of which cybersecurity companies can publish their technical findings is small (Egloff, 2020), nor can the companies fully disclose all the information as it may showcase system vulnerabilities, as it may lead to the aforementioned copycat cases mentioned previously in the paper. The little amount of information that can be fully divulged as well as the small scope of cyber incidents that cybersecurity companies are willing to investigate and be contracted under, leads to a skewed public perception of public attribution cases (Egloff, 2020). This skewed perception of public attribution is a hindrance to norm creation in regard to cyberspace, however, this paper argues that this is only the case as the general analysis of cyber incidents for many years since its inception has been based upon only utilizing technical data as proof of guilt. The recent waves of public attribution have started to shift from the sole release of technical proof to a more holistic approach that involves the standards of proof from the legal profession.

The NotPetya case would be emblematic of this turning point as well as the major case study of the paper's final section. In 2017, an extremely destructive worm named NotPetya attacked several businesses under the guise of a cybercriminal ransomware. The worm, however, was not a simple ransomware, but rather a wiper worm (McKee and McFarland, 2017; Egloff, 2020) that irreversibly encrypted information at the computer's master boot records (McKee and McFarland, 2017; EU Cyber Direct, 2017). Its original target was noted to be Ukraine, however, it affected sixty-four

[12] Sony Pictures Entertainment in 2014
[13] Cybernetic intrusion of the Democrat National Committee in 2016
[14] NotPetya Case of 2017

countries, among them: the United States, Russia, and Brazil[15] and caused what is estimated to be more than 10 billion dollars in damages worldwide (EU Cyber Direct, 2017). The program that was the initial springboard of the worm spread was the Ukrainian program M.E. Doc (EU Cyber Direct, 2017; Ghosh, 2017) and was created utilizing an exploit, EternalBlue[16], allegedly developed by the United States National Security Agency (NSA) (EU Cyber Direct, 2017; Grossman, 2017).

Investigations in the following months by several institutions such as the CIA (Central Intelligence Agency) traced and attributed the NotPetya worm to Russia (Volz and Young, 2018; Nakashima, 2018). The public attribution and subsequent denouncing of Russia was done not only by Ukraine and the United States, but several countries such as Canada, United Kingdom, Australia, New Zealand[17] (Egloff, 2020), Denmark, Lithuania, and Estonia blamed Russia (EU Cyber Direct, 2017). The significance of this event is clear to see when looking at the widespread attribution, political momentum led to various countries to rally behind a flag with the United States not only enacting sanctions against Russia (BBC, 2018), but also indicting six Russian citizens who were allegedly behind the attack[18]. While it has not been at the same moment in time, the European Council came with a list of Sanctions against Russia for the NotPetya attack[19].

The use of public attribution and condemnation by the Five-Eyes Alliance provided momentum towards the molding of acceptable conduct within the space (Egloff, 2020). NotPetya became an emblematic case as not only did the attribution was so strong, but that it can be considered the start of customary law as sets precedent. The attributional factor, that impeded the localization of the source of action, made it nearly impossible to set such precedents before even when looking at the cases with cybercriminals and recreational hackers as their cases had no precedential value (Brown and Poellet, 2012). In itself, the NotPetya case coupled with the subsequent actions set a precedent, though it does also open a few debates of LOAC that are outside the scope of this paper, such as the status of civilian data of which is not covered by the Tallin Manual (Graboritz et. al., 2020).

Both the United Kingdom and the United States have recognized the importance of public attribution and prudent examination of such cyber incidents as methods and tools to influence (Brown and Poellet, 2012; Egloff, 2020). Actions undertaken by States, can and are interpreted by the international community as signals, which point to the direction of where customary laws in cyberspace should take. However, it does not mean that there will be a hard codification of customary laws, as observations of decades of codification of customary laws have been rather mixed with

[15] https://www.businessinsider.com/petya-cyberattack-hit-64-countries-no-kill-switch-2017-6.

[16] EternalBlue created a backdoor into all Windows 8 and older Systems, allowing a Null Session that allowed the client to send commands to the infected server (Grossman, 2017).

[17] These five countries are part of what is called the Five-Eyes Alliance (Egloff, 2020).

[18] See: UNITED STATES DISTRICT COURT WESTERN PENNSYLVANIA (United States). Criminal No. 20-316. [S. l.], 15/10/2020.

[19] The sanctions were not simply against Russia due to NotPetya, but a host of different cyberattacks conducted by Russia and China.

various codifications taking different forms of merely restating customary laws in legislatively non-binding language while others take forms of legislative binding treaties that have a lesser overall adherence (Bordin, 2014).

Whichever would be the case for cyberspace customary laws, what is important to take away from this is the observation that public attribution in cyber incidents have taken on a normative function. This function seeks to create constraints that will become legally binding in various international forums, including international organizations as well as international courts. However long it might take, the political momentum expressed in the NotPetya case shows that there is a clear understanding on the role that international norms and regimes in regard to cyberspace will take, prompting highly influential States, such as the United States, and its allies to start releasing more public attributions.

6. CONCLUSION

As a domain that expanded itself exponentially vertically and horizontally, cyberspace has gained priority in the agenda of many States in the world, often to the point of becoming part of national security. Despite all this, there has not been a customary law that has been consistent in addressing cyber incidents between States in a diplomatic and legal fashion due to early issues regarding the nascent domain such as technical proving and lack of a procedural or criminal international law regarding unsavory acts conducted in this space. Though as this paper shows, during the three decades that cyberspace has existed many changes have been enacted, often leading to progress in the technological, legal and political field that now leave a fertile ground for the foundation of customary laws to be created.

As a result of these changes, there will inevitably be an observation in the rise of public attribution of cyber incidents and States being condemned for not taking responsibility for destructive acts enacted by State agents or non-State actors residing in the accused States. Cyberspace, once an extremely unknown and grey domain, is starting to become a domain that is ordered and with certain laws to mediate conflicts in this dimension. The process, while nascent, is an important one that will lead to great changes in political relations in this intangible domain that connects everyone.

*Artigo recebido em 11 de dezembro de 2020,
aprovado em 13 de abril de 2021.

REFERENCES

BBC. BBC. US imposes new Russia sanctions over cyber-attacks. **BBC News**, [S. l.], p. 1-2, 11 jun. 2018. Available at: https://www.bbc.com/news/world-us-canada-44446449. Access in: 28 mar. 2021. Accessed on: 10 Jun. 2021.

BORDIN, Fernando Lusa. REFLECTIONS OF CUSTOMARY INTERNATIONAL LAW: THE AUTHORITY OF CODIFICATION CONVENTIONS AND ILC DRAFT ARTICLES IN INTERNATIONAL LAW. **The International and Comparative Law Quarterly**, [*s. l.*], v. 63, n. 3, p. 535-567, July 2014. Available at: https://www.jstor.org/stable/43301622. Accessed on: 10 Jun. 2021.

BROWN, Gary; POELLET, Keira. The Customary International Law of Cyberspace. **Strategic Studies Quarterly**, [*s. l.*], v. 6, n. 3, p. 126-145, Fall 2012. Available at: https://www.jstor.org/stable/26267265. Accessed on: 10 Jun. 2021.

CAVELTY, Myriam Dunn; WENGER, Andreas. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. **Contemporary Security Policy**, [s. l.], v. 41, ed. 1, p. 5-32, 14 out. 2019. Available at: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855. Accessed on: 10 Jun. 2021.

CAVELTY, Myriam Dunn et al. The normalization of cyber-international relations. In: CAVELTY, Myriam Dunn. **Strategic Trends 2015: Key Developments in Global Affairs**. ETH Zurich: [s. n.], March 2015. p. 81-98. Available at: https://www.researchgate.net/publication/274076687_The_Normalization_of_Cyber-International_Relations. Accessed on: 10 Jun. 2021.

CHANG, Lennon YC; GRABOSKY, Peter. The governance of cyberspace. In: DRAHOS, PETER (ed.). **Regulatory Theory**: Foundations and applications. [S. l.: s. n.], 2017. p. 533-551. Available at: http://www.jstor.com/stable/j.ctt1q1crtm.42. Accessed on: 10 Jun. 2021.

Charter of the United Nations, Chapter VIII, Article 52. 1945. Available at: https://legal.un.org/repertory/art52.shtml. Accessed on: 10 Jun. 2021.

COPYRIGHT ACT. Act nº N/A, de 1 de janeiro de 1970. N/A. **THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998**, [*S. l.*]: The Government of Japan, n. 48, 1970. Available at: https://www.wipo.int/edocs/lexdocs/laws/en/jp/jp081en.pdf. Accessed on: 10 Jun. 2021.

EASTTOM, C. An Examination of the Operational Requirements of Weaponised Malware. **Journal of Information Warfare**, Peregrine Technical Solutions, v. 17, n. 2, p. 1-15, Spring 2018. Available at: https://www.jstor.org/stable/26633150. Accessed on: 10 Jun. 2021.

EGLOFF, Florian J. Contested public attributions of cyber incidents and the role of academia. **Contemporary Security Policy**, [s. l.], v. 41, ed. 1, p. 55-81, 12 out. 2019. Available at: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324. Accessed on: 10 Jun. 2021.

EU CYBER DIRECT. EU Cyber Direct. NOT PETYA. **Cyber Policy Institute**, [s. l.], p. 28-31, June 2017. Available at: https://eucyberdirect.eu/wp-content/uploads/2020/11/2017-notpetya.pdf. Accessed on: 10 Jun. 2021.

EUROPEAN COUNCIL. European Union. COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020: amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. **THE COUNCIL OF THE EUROPEAN UNION**, [S.

l.], p. 1-2, 20 Jun. 2020. Available at: https://www.legislation.gov.uk/eudn/2020/1127. Accessed on: 10 Jun. 2021.

GRABORITZ, Beth D. et al. Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data. **The Cyber Defense Review**, Army Cyber Institute, v. 5, n. 3, p. 121-132, Fall 2020. Available at: https://www.jstor.org/stable/26954876?seq=1#metadata_info_tab_contents. Accessed on: 10 Jun. 2021.

GHOSH, Shona. The massive 'Petya' cyberattack has hit 64 countries so far and there's no kill switch this time. **Business Insider**, [S. l.], p. 1-2, 28 jun. 2017. Available at: https://www.businessinsider.com/petya-cyberattack-hit-64-countries-no-kill-switch-2017-6. Accessed on: 10 Jun. 2021.

GILES, Keir; HAGESTAD, William. **Divided by a Common Language: Cyber Definitions in Chinese, Russian and English**. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT, 5., 2013, Tallin. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English ... [S.l.: s.n.], 2013. p. 1-17. Available at: http://conflictstudies.org.uk/files/Cyber_Common_Language.pdf. Accessed on: 10 Jun. 2021.

GROSSMAN, Nadav. EternalBlue: Everything There Is To Know. **Check Point Research**, [S. l.], p. 1-2, 29 set. 2017. Available at: https://research.checkpoint.com/2017/eternalblue-everything-know/. Accessed on: 10 Jun. 2021.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, [s. l.], v. 53, n. 4, p. 1155-1175, 2009. Available at: https://www.jstor.org/stable/27735139. Accessed on: 10 Jun. 2021.

HEGINBOTHAM, Eric et al. Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities. In: HEGINBOTHAM, Eric et al**. The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017** . [S.l.]: RAND Corporation, 2015. cap. 11, p. 259-283. Available at: https://www.jstor.org/stable/pdf/10.7249/j.ctt17rw5gb.19.pdf?refreqid=excelsior%3A9a9d8e52666b01ef6f71a2f0a59ab08b. Accessed on: 10 Jun. 2021.

KALLBERG, Jan et al. The Unfitness of Traditional Military Thinking in Cyber. **IEEE Access**, [S. l.], v. 5, p. 8126-8130, 7 jun. 2017. DOI 10.1109/ACCESS.2017.2693260. Available at: https://www.researchgate.net/publication/316078615_The_Unfitness_of_Traditional_Military_Thinking_in_Cyber. Accessed on: 10 Jun. 2021.

LOBATO, LUÍSA CRUZ et al. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, [s. l.], v. 58, n. 2, p. 23-43, December 2015. DOI https://doi.org/10.1590/0034-7329201500202. Accessed on: 10 Jun. 2021.

ICRC, Customary IHL Database Available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule8#refFn_49A37214_00001. Accessed on: 10 Jun. 2021.

PORCHE, Isaac R.; SOLLINGER, Jerry M.; MCKAY, Shawn. **A Cyberworm That Knows No Boundaries** . [S.l.]: RAND Corporation, 2011. 19 p. Available at: https://www.jstor.org/stable/pdf/10.7249/op342osd.8.pdf?refreqid=search%3A43ceee3d8206d1081a1dcbe33afe0f8b. Accessed on: 10 Jun. 2021.

MCKEE, Douglas; MCFARLAND, Charles. Petya More Effective at Destruction Than as Ransomware. **McAfee**, [S. l.], p. 1-2, 30 jun. 2017. Available at: https://www.mcafee.com/blogs/enterprise/petya-effective-destruction-ransomware/. Accessed on: 10 Jun. 2021.

MEJIA, Eric F. Act and Actor Attribution in Cyberspace:: A Proposed Analytic Framework. **Strategic Studies Quarterly**, [s. l.], v. 8, n. 1, p. 114-132, 2014. Available at: https://www.jstor.org/stable/10.2307/26270607. Accessed on: 10 Jun. 2021.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. **Contexto Internacional**. The Fundamental Conceptual Trinity of Cyberspace, [s. l.], v. 42, n. 1, Jan./Apr 2020. DOI https://doi.org/10.1590/s0102-8529.2019420100002. Accessed on: 10 Jun. 2021.

NAKASHIMA, Ellen. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. **Washington Post**, [S. l.], p. 1-2, 12 jan. 2018. Available at: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html. Accessed on: 10 Jun. 2021.

SAGAN, Scott D., WALTZ, Kenneth N. **The Spread of Nuclear Weapons**SMEETS, Max. How Much Does a Cyber Weapon Cost? Nobody Knows. **Council on Foreign Relations**, [S. l.], p. 1-2, 21 nov. 2016. Available at: https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows. Accessed on: 10 Jun. 2021.

SCHMITT, M. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. Cambridge: Cambridge University Press, 2013.

STEVENS, Tim. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. **Contemporary Security Policy**, [s. l.], v. 33, ed. 1, p. 148-170, 13 abr. 2012. Available at: https://doi.org/10.1080/13523260.2012.659597. Accessed on: 10 Jun. 2021.

SINGER, P.W; FRIEDMAN, Allan. **Cybersecurity and Cyberwarfare**: What Everyone Needs to Know. New York: Oxford University Press, 2014. Accessed on: 10 Jun. 2021.

TANCZER, Leonie Maria. 50 shades of hacking:: How IT and cybersecurity industry actors perceive good, bad, and former hackers. **CONTEMPORARY SECURITY POLICY**, [s. l.], v. 41, n. 1, p. 108-128, 24 set. 2019. Available at: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1669336. Accessed on: 10 Jun. 2021.

UNITED STATES DISTRICT COURT WESTERN PENNSYLVANIA (United States). **Criminal No. 20-316**. [S. l.], 15/10/2020. Disponível em: https://www.justice.gov/opa/press-release/file/1328521/download. Accessed on: 10 Jun. 2021.

U.S. COPYRIGHT OFFICE SUMMARY. Act nº N/A, de 1 de dezembro de 1998. N/A. **THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998**, [*S. l.*], 1998. Available at: https://www.copyright.gov/legislation/dmca.pdf. Accessed on: 10 Jun. 2021.

VOLZ, Dustin; YOUNG, Sarah. White House blames Russia for 'reckless' NotPetya cyber attack. **Reuters**, [S. l.], p. 1-2, 15 fev. 2018. Available at: https://www.reuters.com/article/us-britain-russia-cyber-usa-idUSKCN1FZ2UJ. Accessed on: 10 Jun. 2021.