Regulating States Cyber-Behaviour: Obstacles for a Consensus

Marcelo Malagutti
Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). Mestre em Estudos de Guerra pelo King's College London. Pesquisador Sênior do Instituto Vegetius.

Abstract

What are the leading obstacles to reaching a consensus on international norms that regulate state-sponsored cyber-offences? This type of operation increases swiftly, whilst issues related to international law go unnoticed, are poorly understood, or are manipulated, clouding the debate on norms of international conduct in cyberspace. This article analyses the main obstacles to regulating such cyber--offences. It argues that the main difficulties concern statecraft and state power promotion, not novelty or innovation speed, ideological or technological issues, as usually claimed. The analysis encompasses the applicability of the current rules of armed conflicts to the cyberspace context, the perspectives and positions regarding multilateral conventions, the option for bilateral or regional agreements and the *normalisation* of some cyber-activities as means of influencing consuetudinary law. It is shown that some nations advocate for maintaining the *status quo* that favours them, whilst others insist on the need for specific regulations.

Keywords: International Norms; Cyber--Behaviour; Interstate Conflicts.

Resumo
Regulação do Comportamento Cibernético dos Estados: Obstáculos para um Consenso

Quais os principais obstáculos para um consenso sobre normas internacionais que regulem as ciberofensas patrocinadas por Estados? Esse tipo de operação cresce rapidamente, enquanto questões relacionadas ao direito internacional passam despercebidas, são mal compreendidas ou manipuladas, ofuscando o debate sobre normas internacionais de conduta no ciberespaço. Este artigo analisa os principais óbices para essa regulação. Argumenta que as principais dificuldades dizem respeito ao estadismo e incremento do poder estatal, e não à novidade ou à velocidade da inovação, questões ideológicas ou tecnológicas, como comumente se afirma. A análise engloba a aplicabilidade das regras atuais de conflitos armados ao contexto cibernético, as perspectivas e posições relativas às convenções multilaterais, a opção por acordos bilaterais ou regionais e a normalização de algumas ciberatividades como meio de influenciar o direito consuetudinário. Mostra-se que algumas nações defendem a manutenção do status quo que as favorece, enquanto outras insistem na necessidade de regulamentações específicas.

Palavras-chave: *Normas Internacionais; Comportamento Cibernético; Conflitos Inter*estatais.

Artigo recebido: 25.07.2022
Aprovado: 12.12.2022
https://doi.org/10.47906/ND2022.163.05

Introduction

In February 2018, the UN Secretary-General expressed twice his concern about the absence of specific international norms to regulate cyber conflicts. He repeatedly used the words *cyberwar* and *cyberattacks* and stated that 'episodes of cyber warfare between states already exist', that 'there is no regulatory scheme for that type of warfare' and that 'we have not yet been able to discuss whether or not the Geneva Conventions apply to cyberwar or whether or not international humanitarian law [IHL] applies to cyberwar' (Guterres, 2018; Khalip, 2018).

What are the obstacles to reaching a consensus on international norms regulating state-sponsored cyber-offences? For this article, these offences consist of more 'peacetime' (or even 'grey zone') operations, such as intelligence gathering (either surveillance or espionage), coercion and influence cyber operations, and more traditional military objectives, such as power projection, area denial, disruption and force multiplier (Malagutti, 2016). Accusations of these operations increase swiftly (Hollis et al., 2020; Nathan and Scobell, 2020). The article analyses recent initiatives on the international regulation of interstate activities in cyberspace and the difficulties in reaching a consensus on common rules. Arguments used in various initiatives are analysed, based on official documents, and academic and international news articles, in an attempt to identify different perspectives. The research deconstructs the arguments, usually found in official speeches and academia, that the problem stems from ideological, technological, novelty or speed of innovation issues. It concludes that the difficulty in regulating cyberspace is exclusively geopolitics, as usual, in its sense of the study of spaces in international politics and the production of knowledge to subsidise statecraft and promote the power of states (Tuathail and Agnew, 1992). Subjacent to the arguments repeatedly used by different countries in multilateral forums, there is a geopolitical struggle; while western powers try to maintain the *status quo* of the technology gap that favours them, there is firm resistance on the part of their opponents to buy time to organise their internal environments and to limit the disadvantages and risks posed to them by this gap.

On the Foundations of International Laws Development

Article 38 of the statute of the International Court of Justice (ICJ) lists the sources of international law. International conventions are the first, establishing rules expressly recognised by signatory States. Then, there is international custom, as evidence of a general practice, accepted as law, and 'general legal principles recognised by civilised nations'. In another group, as subsidiary means, are judicial decisions and

the doctrine 'of the most qualified lawyers from different nations' (UN, 1945). Nevertheless, the 'advent, over the last decades, of new actors at the international level, has contributed to expanding how international law has come to manifest itself', and Article 38 'never intended to constitute a peremptory and exhaustive formula from the sources of international law, but only as a guide to the activity of the International Court' (Cançado Trindade, 2017).

Although not expressly written, customary law (international customs) is binding similarly to treaties. It is consolidated under the influence of two elements: one objective, which consists of practice (the *usus*); and another subjective, which consists of the belief that the action was taken in the form of an obligation (the *opinio juris*) (Schmitt and Vihul, 2014). Despite the large number of international treaties signed in recent decades, customary law remains relevant because even nations that are not signatories to certain treaties generally follow them. For example, even though the USA and Israel are not part of the 1977 Additional Protocols to IHL, they generally respect its rules (Schmitt and Vihul, 2014). In the absence of international conventions, States that manage to establish (or demonstrate) the existence of customs, an international practice, or even create specific doctrines, may influence international regulation in the future. As will be seen, such a future is not necessarily a distant one, and some States are endeavouring to seek to meet conditions for this.

On the (False) Novelty of 'Cyber-Things'

A justification frequently used for the absence of a legal *corpus* suitable for cyberspace refers to the novelty of technologies and their use. The adequacy of the International, political, and legal systems to new technologies often comes after a long time of assimilation; thus, considering the novelty of cyber-activities, few treaties deal specifically and directly with the topic (Toffler, 1991; Schmitt and Vihul, 2014). Similarly, Joseph Nye (Nye, 2018) argues that the first international cooperative agreements of the nuclear era took more than two decades to be signed, and that if cyberspace is considered 'not since its creation in the early 1970s', but from 'its dissemination since the late 1990s', then it would be taking a similar term. Note the proposed 'adjustment', cutting almost three decades (from the early 1970s to the late 1990s) to corroborate his comparison with nuclear agreements.

Despite, typical examples of international 'cyber-treaties' are the 1992 Convention and Constitution of the International Telecommunications Union (ITU) and the 1992 International Telecommunications Regulations, the 2001 Convention on Cybercrime (the Budapest Convention), its 2006 Additional Protocol, and the 2008 Shanghai International Cooperation Organization Information Security Agreement

(Schmitt and Vihul, 2014). It shall be noted that, among the examples cited, the 1992 Conventions are almost three decades old, while the Budapest Convention on Cybercrime dates from nearly two decades. Besides, the first known case of military technology cyber-theft from American universities by foreign agents occurred already in 1989 (Stoll, 1990). Thus, iconic cases started in the early 1990s, as well as the negotiation of international norms. Hence, 'neither cyber-conflict nor legal arguments about it can be remotely described as new concepts' (Giles and Monaghan, 2014). Therefore, the argument of novelty does not prosper.

Moreover, historically, international consensus is achieved quickly in other regulatory contexts, such as that of contagious diseases; in the severe acute respiratory syndrome (SARS) epidemic, the World Health Organization issued norms, both binding and non-binding, to allow the control of the spreading virus (Finnemore and Hollis, 2016; Fidler, 2003). In 2005 these norms were consolidated under the new International Health Regulations (IHR) (Nunes, 2017). The example of the 'immediate customary law' also weighs against the novelty argument. In 1963, the UN General Assembly approved the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, without any previous regulation, or even tradition, based only on the tacit agreement between the two only relevant space actors of the time, the USA and the USSR (Cançado Trindade, 2017). That debate reflected divergent positions between the two superpowers as to the best regulatory alternative (as it happens in the case of the cyber-norms, indeed), but a 'pragmatic' agreement was achieved:

> [...] while the then USSR preferred a treaty, the USA insisted on a General Assembly resolution, a formula that the USSR was finally persuaded to accept given the complicated and politically uncertain procedure of concluding treaties under USA constitutional law (Cançado Trindade, 2017).

The International Committee of the Red Cross (ICRC) stated in a position paper that the ICJ's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons recalled that the established principles and rules of IHL applicable in armed conflict apply 'to all forms of warfare and to all kinds of weapons', including 'those of the future' (ICRC, 2019). Therefore, for the ICRC, any new law must comply with those principles.

Whilst the novelty argument does not subsist, a genuine obstacle to the consensus regards the terminology adopted. In international law, it can qualify or disqualify the application of a particular norm. The term cyberwar could have a different receptivity if replaced by *cyber-armed conflict*, or even *conflict with cyber weapons*. In the UN Charter, the word *war* appears only in the preamble, whether the Geneva Conventions adopted the generic expression *international armed conflicts*, due to 'the large number of wars that were not considered as such' (Pereira, 2010).

Another conflicting term among the legal community is attack. *Armed attack* is a legal term established in *jus ad bellum* and IHL. The term is defined in Article 49 of the Additional Protocol to the Geneva Conventions, as consisting of acts of violence against an opponent, both offensive and defensive. The definition of *attack* lies at the heart of IHL; many of the bans are defined in terms of the ban on attacks, the paradigmatic example being that of attacks on civilians or civilian objects (Schmitt and Vihul, 2014). However, there is no widely accepted definition of what a cyberattack is. Definitions vary from 'unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems' to 'a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization' or actions that 'aim to damage or gain control or access to important documents and systems within a business or personal computer network' (IBM, n.d.; CISCO, n.d.; Microsoft, n.d.)

On the Distinctive Perspectives Regarding Cyberspace and Its Regulation

Two opposing views concentrate the clash over the regulation of States' behaviour in cyberspace. 'Western democracies', mainly the USA and its closest allies, push for a more open Internet concerning individual freedom of expression, while others, such as Russia and China, insist on the importance of sovereign control of cyberspace (Nye, 2018). Nonetheless, there is controversy even on the very nature of cyber-conflicts. The USA understands cybersecurity as the protection of hardware, software and information. Conversely, China and Russia favour the concept of 'information security', which allows the State to control online content to preserve the stability of their regimes (Grigsby, 2017). Such differences, in practice, have been the 'apple of discord' that hampers the consolidation of international law on state-sponsored cyber-offences.

A superficial analysis of the official arguments would indicate that the western powers defend individual rights and free business in cyberspace, the very foundations of the creation of the Internet itself, whilst Russians and Chinese aim at surveilling their citizens and protecting their regimes. This antagonism is impregned with the view of the 'Western' liberal world order implemented after WWII under the leadership of the United States (Barrinha and Renard, 2020). Such a simplification hides other relevant aspects and makes other countries' positions somewhat ambiguous. Brazil, for instance, has internal laws that largely reinforce net neutrality and the protection of individual privacy, but resists the USA diplomatic line regarding international regulation. In what starts to be called 'post-liberal order', the 'liberal-order' is challenged not only by the China-Russia-led group, but also by

the then U.S. President Trump's view of multilateralism and his commercial war on China; it is also confronted by opinions expressed by the Hungarian, Polish and Brazilian governments (Barrinha and Renard, 2020).

The Huawei case exemplifies illiberal actions promoted by a post-liberal West. The USA accuses Huawei, the world leader in 5G telephony, of having obscure connections with Chinese intelligence. The USA argues that it prefers the use of equipment from the Swedish Ericsson and Finnish Nokia, although more expensive, and personalities of the Trump Administration have even suggested the acquisition of the control of these companies (Kharpal, 2020). The USA also pressure its allies to veto the use of Chinese technology. In May 2020, the UK reformed a previous authorization of limited Huawei participation in British networks, and announced a complete ban on the company. The German Deutsche Telekom (32% state-owned) posed that excluding Huawei from its networks would be 'Armageddon'. Despite, although not restricting its participation, it recently announced that Ericsson was chosen as its 5G supplier (Petzinger, 2020; Alleven, 2020; Ericsson, 2020). Similarly, France decided not to ban Huawei from its networks, but 'encourage' their telecom companies to avoid it (Rose and Harvey, 2020). Under enormous pressure from the USA regarding the participation of Huawei in Brazilian networks, with the U.S. ambassador threatening 'consequences', in a very pragmatic position, the Brazilian military reportedly told their government that 'the same eventual exposure that Brazil may suffer from Chinese technology with Huawei will also occur with any other company' (Amado et al., 2020; Rosa and Antunes, 2020).

In a similar take, in the early stages of the COVID-19 pandemic, when the German company CureVac announced promising results in its research for the development of a vaccine, the U.S. government offered advantages to the company if it moved its research to the U.S., provoking immediate reaction of the German government (Morris, 2020; Carrel and Rinke, 2020). Albeit elucidative of current inter-State competition, this last example does not relate to cyberspace. Nonetheless, the pandemic also provides examples of fierce competition in the cyber realm. The COVID-19 'vaccine nationalism' increased the scale of cyberespionage actions targeting vaccine R&D promoted by intelligence agencies from many countries (Fidler, 2020). Specialists argued for the applicability of international law to cyberattacks targeting the healthcare sector and vaccine research and even argued that vaccine installations configure critical infrastructure, although not explicitly addressing cyber espionage (Fidler, 2020).

The aforementioned cases constitute clear and fresh evidence of increasing competition not only among rivals, but also among traditional western allies. Therefore, it is not the case of considering the different views regarding international norms for cyberspace a simple question of different ideological positions of the 'west and the rest', becoming necessary to analyse the context with other lenses. One could

argue that the 'west' is only reacting in the same way it has suffered in recent years. To tackle this argument, it is necessary to go back in time.

Despite Russian agents' apparent (or even likely) use of Twitter and Facebook for disinformation campaigns, using social networks for political purposes was not a Russian invention. In June 2009, the U.S. Secretary of State Hillary Clinton asked Twitter to postpone a programmed update of the app, which would leave it unavailable for a few hours during the final phase of Iran's election campaign. She claimed that the app was enabling a revolution in that country. On the same day, President Obama said that 'people's voices should be heard and not suppressed in Iran'. The company postponed that planned maintenance, but the Iranian government-supported candidate won the elections easily (Plening, 2009; Nuttall and Dombey, 2009).

Albeit the Iranian case, the Russians claim that other western interference cases succeeded. They argue that the Gaddafi government failed to control social media in Libya, leaving great freedom of action to its opponents, which led to military support from the USA and NATO, ultimately allowing the fall of the regime and culminating in the civil war in Libya (Giles and Monaghan, 2014). The 'Arab Spring', which led to the fall of regimes in Tunisia (2010) and Egypt (2011), would also have been greatly influenced by social network actions promoted by western intelligence agencies. Similarly, in Syria, protests promoted in these networks in January 2011 evolved into a violent civil war that persists until today, with the direct engagement of the USA and Russia on opposite sides. Sergei Smirnov, Deputy Director of the FSB (Federal'naya Sluzhba Bezopasnosti, or Federal Security Service of the Russian Federation), the successor of the famous KGB (Komitet Gosudarstvennoy Bezopasnosti, or Committee for State Security), declared in 2012: 'new technologies are used by Western secret services to create and maintain a level of continuous tension in society with serious intentions, even reaching a regime change' (Giles and Monaghan, 2014). Therefore, Russian concerns regarding the misuse of social media must be analysed in the context of this perception of existential threat, not merely ideological paranoia (Giles and Monaghan, 2014).

During the Cold War, when the world was ideologically divided into two blocs, a leading American strategist defined the USA as a *status quo* nation, 'determined to keep what it has, including existence in a world of which half or more is friendly or at least not sharply and perennially hostile' (Brodie, 1959). With the fall of the USSR, the USA became an unchallenged superpower, no longer interested only in half of the world.

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

The U.S. software industry is the largest in the world, being a net exporter and concentrating many of the best programmers in the world; computer courses at their universities are ranked at the top; the Pentagon has been working on public-private partnerships to build superior military capabilities in cyberspace (Libicki, 2009; Lynn, 2010; Morgan, 2010; Rid and McBurney, 2012; Libicki, 2019). Even though there is considerable secrecy about USA cyber offensive capabilities, it is widely believed that they are probably the best in the world.

Albeit demonstrating some advanced capabilities, and often being accused of cyberattacks against the West, Russians and Chinese are deeply uncomfortable with American cyber policy, seeing it as 'evidence of muscle flexion and dominant behaviour', compounded by the perception of a massive gap comparing USA cyber capabilities with theirs (Austin, 2016). Such a gap, favourable to the 'threatening west', broadens their perception of existential risk, with the consequent need for technologically asymmetric responses, and results from the perception that the gap is too big to be overcome (Giles and Monaghan, 2014).

This technological gap can also be associated with the problem of attribution of cyberattacks. It is well known that attributing cyberattacks is harsh (Buchanan and Rid, 2014; Lupovici, 2014). It is also a fundamental step for the application of international laws of conflict. Nevertheless, it is presumably easier for countries with advanced cyber capabilities, and harder for those with limited ones. Thus, the acceptance of current international law to cyberspace operations would favour those with advanced capabilities, maintaining their *status quo*. And this would also limit their interest in sharing technical information on cyberattacks with the less skilled group, re-feeding the process.

Faced with the perception of a growing threat, the Russian parliament passed a law prohibiting its Internet traffic from being redirected to servers in other countries, creating what the Western press has called the 'Internet Iron Curtain' (Deutsche Welle, 2019; BBC, 2019). For their part, the Chinese implemented *The Great Firewall of China* (Raud, 2016).

On the other hand, the Western feeling of Russia as a constant threat to the stability of the West is reinforced by the view that cybercrime is rampant in Russian cyberspace, leading many to conclude that the government of that country is in collusion, a perception aggravated by the country's non-accession to the Convention of Budapest on Cybercrime. This feeling partly stems from the little publicity (in the western media) of the efforts against cybercrime in Russia. Even these efforts are perceived in the West as attempts to control the freedom of expression and censorship of the Internet, even if they are in accordance with corresponding international norms (Giles and Monaghan, 2014).

The Russian perception of vulnerability increases their usual emphasis on international norms as the essential framework underpinning all interstate activity, and

partly explains the Russian persistence in the search for international normative instruments to govern cyberspace (Giles and Monaghan, 2014). Russia's primary objective concerning cyberspace norms has been the promotion of a treaty that could limit the development of cyber-weapons or the use of cyber means to interfere in the internal affairs of other states. Fundamentally, they argue that new technologies demand new laws that guide States to use them peacefully (Grigsby, 2017). The Chinese argue the same (Huang and Mačák, 2017). The USA opposes; initially, arguing that the 'information security' view could legitimise censorship by authoritarian governments, what 'would be unacceptable for democratic governments'; subsequently, claiming that such a treaty would be unverifiable (Nye, 2015, 2018).

Treaties require the express consent of States. Gary Corn, a former USCyberCom legal adviser, notes that the basic principle of any negotiation is that 'no one negotiates against himself' (Daskal et al., 2019). Insofar having strategically or operationally useful capabilities, some States have no incentive to limit the option of using them (Mačák, 2016). These same countries, however, are also vulnerable to hostile operations by other states with similar or even lower capabilities. Therefore, different bodies in the same country see national interests from different perspectives and may differ in how that country should characterise a particular practice (Schmitt and Vihul, 2014). Despite, while the rationale points to a net advantage of the pros facing the cons, the case in favour of the maintenance of strategic advantage prevails.

It turns out that these different perspectives are not limited to the mentioned countries, extending to their respective allies and even to countries not naturally aligned with one or the other group, but who feel threatened by the positions of both groups. This *split*, essentially guided by the different pragmatic views of the use of the Internet as a weapon of power, a tool for statecraft, or an instrument for free dissemination of information and expression, can better explain the difficulty of obtaining consensus, or even of implementing what has already been agreed.

On the Applicability of The Current Armed Conflicts Law

A key issue in the debate is the applicability of the current *jus ad bellum* and *jus in bello* to cyberspace activities. On the one hand, it is argued that, in the absence of specific rules, states should work by analogy, either by equating cyberattacks to traditional armed attacks and treating them under the laws of war or by equating them to criminal activities and dealing with them in the manner of internal criminal laws (Sklerov, 2010). The USA and its allies, particularly in NATO, favour this argument, even though some fundamental principles remain unresolved, such as

what would be a cyberattack or characterise the use of force in cyberspace. On the other hand, Russia, China and Brazil, among others, express considerable reluctance to agree with the applicability of non-specific rules, considering the need for specific agreements as an imperative (Schmitt and Vihul, 2014; Giles and Monaghan, 2014).

It was in the context of the applicability of the current rule that, under the auspices of NATO, an international group of academics produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013). The work was expanded with the 'Tallinn 2.0' Project, published four years later, full of examples that illustrate an interpretation of the application of current rules to cyber operations (Schmitt, 2017). The Chinese often argue that the initiative is a clear example of an attempt to legalise military use of cyberspace by western powers (Henriksen, 2019; Huang and Mačák, 2017).

Although the doctrine is a secondary source of international law, it constitutes a 'highly persuasive' element in the interpretation of the provision of treaties and the identification of international custom. A doctrine common to several states can evolve into a 'general legal principle recognised by civilised nations', and later develop into a custom. Therefore, in the absence of conventions or customs related to cyber-conflicts, academic works such as the Tallinn Manual can be a relevant tool for identifying and formatting legal norms for cyberspace (Schmitt and Vihul, 2014). And this may be contrary to the interests of those who oppose the primacy of the USA.

Since 2010, the USA has been relatively successful in getting some top cyber powers to agree to an increasingly prescriptive set of rules on what they could and could not apply in cyberspace. The process failed, however, in obtaining explicit consent to the applicability of laws of war to cyber-conflicts. Russia, China and Cuba, among others, have refused to do so, ruled by the suspicion that this would constitute a 'green light' for hostile actions in cyberspace (Grigsby, 2017).

Not only traditional USA opposers disagree, however. Even NATO members have worked to shape customary law, expressing different views on fundamental aspects. While the United Kingdom disregards the nature of sovereignty in cyberspace, France defined it clearly (Wright, 2018; France-MdA, 2019). France also disagrees with relevant parts of the Tallinn Manual, for instance, regarding the due diligence principle and actions initiated by non-state actors inside a State against another State (France-MdA, 2019).

Current 'laws of war' establish that a State's recurrent inability to curtail illegal actions in its territory against other States may result in its qualification as a *sanctuary*. Besides, States victimised by armed attacks promoted by non-state actors located in another state can respond by force, when host states violate their duty to prevent such attacks (Pereira, 2010).

If such rules apply to cyberspace, the imputation of responsibility for cyberattacks originating in a State would provide a legal path for others to use active defences (and other offensive capabilities) without the need for conclusively attributing the attack to that State or its agents (Sklerov, 2010). This configures a good reason for countries where cybercrime is rampant, like Russia and Brazil, to privilege the elaboration and application of internal laws before recognising the applicability of international armed conflict laws to cyberspace.

Moreover, both the USA and the Netherlands recently adopted an understanding that the use of force defensively in the cyber realm is permitted under the auspices of Article 51 of the UN Charter, even if a cyberattack by a non-state actor cannot be formally attributed to another state. It is unclear when a cyberattack will be severe enough to be considered an armed attack in the sense provided for that article. According to the Tallinn Manual, cyber operations that cause 'significant' damage, destruction, injury or death qualify as such (Schmitt and Vihul, 2014). Significant, however, remains a subjective concept.

Finally, despite the American insistence that current international regulations apply to cyberspace, for which States should not knowingly attack critical infrastructures in other States, in 2010, the USA and Israel allegedly used Stuxnet to compromise uranium enrichment facilities in Iran. Different experts considered such action to be an illegal act of violence under international law (Zetter, 2013).

On the Perspectives of a 'Digital' Multilateral Convention

In November 2019, the UN Assembly approved two separate proposals to debate the regulation of cyberspace activities: one from the USA, creating a Group of Government Experts (GGE); and another from Russia, creating an Open-Ended Working Group (OEWG) (Achten, 2019; Grigsby, 2018; Colatin, 2018).

GGEs are common in the UN routine, constituted *ad hoc* when any subject deserves UN attention, with experts from 15 to 25 countries, but they are rarely successful (Achten, 2019; Nye, 2018). GGEs related to cyber regulation are nothing new. Those of 2004-5 and 2009-10 did not obtain significant results; however, the 2012-13 one had considerable success. For the first time, 15 countries, including Russia, China, the USA, India, the United Kingdom, France and Germany, understood that the *jus ad bellum* (the UN Charter) would apply to cyberspace. However, there was no agreement on *jus in bello* (IHL). The 2014-15 GGE developed new rules to guide the activity of States in cyberspace in times of peace but did not achieve the same success as its predecessor, as intended by the USA (Fidler, 2018; Grigsby, 2017).

Differently, OEWGs are forums open to all nations. The USA opposed this one, arguing that two separate discussion groups would divide efforts and that Russia's

intention was to delay the discussion in a broader forum (Achten, 2019; Grigsby, 2018; Colatin, 2018). However, already in 1998, Russia was the first nation to propose an international UN treaty to ban electronic and informational weapons (including for propaganda purposes), which could be used to 'adversely affect the security of states', with a resolution passed by the Assembly General (Grigsby, 2017; Nye, 2018). In 2011, Russia, China, Tajikistan and Uzbekistan proposed rules at the UN to regulate 'the dissemination of information incompatible with the domestic policy and the social and economic stability of countries, as well as their cultural and social environment' (Stevens, 2012).

In any analysis, however, the approval of these two groups by the General Assembly shows that international concern with the issue is general and that the arguments of both sides are being heard. This concern is also evident in other initiatives.

In 2011, in London, the Global Conference on Cyberspace (GCCS), also called London Process, was held to establish principles of behaviour on the Internet. The GCCS continued with conferences in Budapest (2012), Seoul (2013), The Hague (2015) and New Delhi (2017). In 2017, the Dutch think tank The Hague Centre for Security Studies (HCSS) announced the creation of The Global Commission on the Stability of Cyberspace (GCSC) with the aim of 'helping to develop norms and policies that promote international security and the stability of cyberspace' (Nederlands-HCSS, 2017). In 2018 GCSC published the Singapore Standard Pack (GCSC, 2018), and in November 2019, issued its final report (GCSC, 2019).

Private companies also promote initiatives. In September 2018, Microsoft launched its Digital Peace campaign, with a set of proposals aimed at protecting the privacy and security of customers in the computer industry. The following month, the German group Siemens, whose software for controlling Iranian centrifuges was targeted by Stuxnet, published its Charter of Trust, seeking adherence to a 'global standard' of cybersecurity (Laudrain, 2018).

In November 2018, France announced the Paris Call, based on the UN Charter and recognising the applicability of IHL to cyber conflicts, as well as international human rights law and customary law in general (Laudrain, 2018). In 2018, the initiative counted 75 countries, 341 civil society organisations and 624 private companies, recognising the relevance of companies and other non-governmental organisations to the stability of cyberspace (France-Diplomatie, 2018; Laudrain, 2018). The absence of the USA, China and Russia as signatories is not surprising, while the absence of Brazil and India may cause the initiative to lose traction (Laudrain, 2018). Although legally non-binding, the initiative tries to establish some basic principles of consensus, which could, in the future, be consolidated in international law (Shackelford, 2019).

Despite the attention paid in the last decade to the international debate on norms, the conclusion of new cyber treaties is unlikely in the short term, given the strong

opposition of Western nations (Schmitt and Vihul, 2014). Some argue that any international treaty on the subject would probably be riddled with reservations, thus degrading its practical effect (Elliott, 2011). This argument can also be factually contested. For example, the Budapest Convention on Cybercrime reached 64 ratifications, with 32 reservations and 29 declarations. Excluding Russia, Ireland and Sweden, all other 44 members of the Council of Europe (EC) joined it, plus non-EC member countries such as the USA, Canada, Japan, Australia and Argentina (Council of Europe, 2019).

Until 2019, none of the BRICS had yet joined the Budapest Convention (South Africa signed it but did not ratify). In December 2019, Brazil announced it started its accession to it (Brasil-MRE and Brasil-MJSP, 2019). This accession was concluded only in November 2022. Historically, Brazil used two arguments to justify not joining the Convention. First, 'Brazilian foreign policy privileges the agreements whose drafting Brazil participated in, to place our brand, our interest' (Vital, 2008). It reflects a legitimate concern with the dominance of the great powers in the debate, which is explicit in the statement by the then-Secretary for Combating Transnational Offenses of the Brazilian Ministry of Foreign Affairs:

> In a way, there is a democracy of vulnerability. Both developed and developing countries are in the same pattern. In this sense, Brazil intends not only to react but also to make its own proposals, so that more technologically developed countries do not dominate the debate (BOL, 2011).

This argument is consistent with the notion that treaties are *one*, and not *the*, product of international negotiations; another product is the negotiation process itself; 'The journey matters as much as the destination' (Finnemore and Hollis, 2016). In this process, several components take part: incentives, such as favourable trade agreements; *coercion*, in the form of bribes or threats; *persuasion*, in the search for changing attitudes; and *socialisation*, when countries with asymmetric capacities are considered as equals whose opinion has value (Finnemore and Hollis, 2016). In other words, some countries try to become 'norm-makers' instead of only 'norm-takers' (Reilly, 2012). Not being part of the Council of Europe, sponsor of the Budapest Convention, and thus excluded from the negotiation, Brazil urged for the European text to be discussed under the auspices of the UN (Vital, 2008).

The second argument was that 'what matters primarily is our internal legal system' (Vital, 2008). It reflects a concern with the internal stabilisation of cybercrime before acceding international conventions or recognising their validity, probably related to formal accountability or designation as a *sanctuary*. The official note itself nods in this direction when declaring that 'Brazil's accession initiative to the Budapest Convention comes in addition to Law 12,965/2014, named Marco Civil da Internet, for the criminal prosecution of cybercrimes' (Brasil-MRE and Brasil-MJSP, 2019).

If multilateral agreements cannot be quickly reached, bilateral ones become an option. In 2014, China and the USA agreed that their governments would not conduct or knowingly endure economic cyber-espionage, fulfilling an old objective of the USA in containing Chinese thefts from American companies. Subsequently, bilateral agreements were signed between many G20 members (Grigsby, 2017). In 2015, Russia and China signed a bilateral cooperation agreement in cyberspace, which in addition to reflecting their previous diplomatic positions, innovated with a mutual commitment to non-aggression (Korzak, 2015b, 2015a; Roth, 2015). All of these bilateral agreements lay the foundations for customary law.

On the Difficulties of Customary Law in Cyberspace

A significant impediment to the emergence of customary law is the lack of visibility of what happens in cyberspace. Generally, only the effects of cyberattacks are publicly observed; in many cases, not even these are perceived by the general public. Some victim states avoid revealing cyber incidents since doing so might reveal capabilities considered essential for their security (Schmitt and Vihul, 2014). In the 2014 Sony case, the USA quickly attributed the attack to North Korea, facing widespread scepticism, until the press revealed that the Americans had access to North Korean computer networks (Nye, 2015). The revelation almost certainly 'burned' some USA intelligence sources. Even so, then-President Obama classified the incident as an act of 'cyber-vandalism', a statement with no legal implications under international law (Sander, 2019).

The 'silence' regarding cyber-offences has additional motivations: the desire to maintain some ambiguity that allows them a desired (or necessary?) 'operational flexibility' in cyberspace; the existence of geopolitical interests, possibly not directly related to cyberspace; difficulties of attribution or regarding measures taken in response to cyber-offences; or the desire of not linking such offences to a particular international standard, or to legitimise certain practices of other states (Sander, 2019). States may also wish not to indicate to their opponents when they could resort to the argument of self-defence, or prefer not to make clear their threshold to resort to 'use of force'; remaining silent, they reserve space for some 'strategic ambiguity' (Schmitt and Vihul, 2014). The general nations' silence regarding the Stuxnet case does not mean they considered the operation legal. They may have concluded it was illegal, since it did not occur in response to an armed attack, but that it was more acceptable than a preventive kinetic attack (Schmitt and Vihul, 2014).

Despite, acts not made public do not constitute a customary practice. International custom emerges from the 'interaction of rival claims by States'; 'the State that can cite more precedents will have an advantage over its opponent, regardless of the

mode of peaceful settlement of the dispute, for the consolidation of customary international law' (Cançado Trindade, 2017).

Other requirements for the formation of customs are consistency and density, reflecting the support of other nations. In 2013, in the wake of the Snowden case, Brazil argued within the UN General Assembly that interception of communications represents a case of disrespect for national sovereignty. It is unlikely that a sufficient number of other States will support such a claim to the extent that a customary standard will be established (Schmitt and Vihul, 2014).

Another problem lies in the 'normalisation' of some practices in the cyber context that are contrary to international custom regarding armed conflicts (Libicki, 2019). Literature is full of different threat names: viruses, worms, botnets, Trojan Horses, malware, 'rogue code', logic bombs, and so on. Nevertheless, they all have two things in common: they consist of software, and they must be 'implanted' (installed) in advance on the target networks. Generally, malware implantation takes weeks, even months, in advance for a relevant cyberattack to be successful.

In June 2019, an international crisis unfolded when Iran seized a British oil tanker in the Persian Gulf. The Royal Navy immediately sent a war vessel to prevent subsequent seizures of British ships, in an attitude easily characterised as self-defence under current international norms. Subsequently, it was revealed that the USA carried out cyberattacks that damaged the database used by the Iranians to carry out the arrests, even though no USA vessel had been affected. (Barnes, 2019). The database hack itself configures a preventive action. Furthermore, it probably demanded the use of implants deployed long before.

While the principle of self-defence has a legal provision of customary nature, there is no legal support for preventive actions (Pereira, 2010). The Bush Doctrine, published a year after the 9/11 terrorist attacks, reiterated that the USA has long insisted on the possibility of pre-emptive attacks, and went further advocating for the legitimacy of preventive strikes (Bush, 2002). A pre-emptive attack is carried out when an attack is imminent; a preventive attack is carried out to prevent the enemy from being able to attack in the non-imminent future. Notwithstanding such a differentiation, both are carried out before an enemy attack occurs, and thus cannot be considered self-defence in line with the legally accepted framework (Pereira, 2010).

The threat of retaliation against cyber-offences through kinetic attacks is another practice that became somehow 'normalised', notably by nations such as the USA, the United Kingdom and France. It should be noted, however, that only Israel has used kinetic forces (an air attack) in retaliation against cyberattacks by Hamas hackers, and yet within an existing state of 'war on terror' (Newman, 2019).

All in all, the consolidation of customary law on cyber-conflicts seems more likely from the interpretation of already established customs, in which case interpretive

dilemmas will certainly arise (Schmitt and Vihul, 2014). NATO member nations appear to rely on this scenario, which is why the Tallinn Manual reflects several examples of the application of current international norms to cyberspace situations.

Conclusion

Great Powers achieved some alignment regarding specific basic rules on the applicability of international law to cyberspace. However, attempts to go further, as in obtaining an explicit endorsement for *jus in bello*, still seem distant.

Contrary to common belief, this is not a problem related to the novelty of the topic, nor even ideological issues such as authoritarianism versus the right to privacy. Part of the problem lies in the fact that cyber-conflicts, as they do not directly result in physical effects (destruction or death), are considered 'grey zone conflicts', below the threshold of armed conflict. Therefore, outside the original context of the existing norms. Besides, cyber operations are largely associated with espionage, a practice not regulated in international law on armed conflicts.

Different interest groups stand on opposing sides in the debate, making consolidating comprehensive international law rules challenging. On one side, there is the USA and a large part of NATO member states, interested in maintaining the *status quo*, and taking advantage of their technological edge. On the other side, there are mainly Russia and China, whose cyber technical capabilities (and investments in them) are considerably lower than those of the previous group, despite significant recent advances. The current gap is perceived as limiting their capabilities and leaving them vulnerable if certain interpretations of the current regulatory framework are applied.

In this arm wrestling, the application and interpretative evolution of the existing international regulation, or at least the creation of doctrine and custom, is more likely in the short term, as the Western powers intend, instead of specific new treaties, as desired by Russia, China and Brazil.

Negotiations continue, with nations of the second group gradually making concessions while accelerating their efforts to evolve their internal legal frameworks to make them compatible with the standards of the Western powers, attempting to prevent legal pretexts for actions against them.

References

Achten, N. (2019) New U.N. Debate on Cybersecurity in the Context of International Security. *Lawfare*.

Alleven, M. (2020) Deutsche Telekom selects Ericsson for 5G RAN in Germany. *FierceWireless* [online]. Available from: https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany.

Amado, G. *et al*. (2020) O recado das Forças Armadas ao Ministério da Defesa sobre o 5G – Época. *Época*. [online]. Available from: https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588.

Austin, G. (2016) 'Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security', in *Asian Security Conference 2016*. 2016 p.

Barnes, J. (2019) U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say. *The New York Times*. [online]. Available from: https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

Barrinha, A. & Renard, T. (2020) Power and diplomacy in the post-liberal cyberspace. *International Affairs*. [online] 96 (3), 749-766.

BBC (2019) Russia internet: Law introducing new controls comes into force. *BBC News* [online]. Available from: https://www.bbc.co.uk/news/world-europe-50259597

BOL (2011) Itamaraty pede política global no combate a crimes cibernéticos. *BOL Notícias*. [online]. Available from: https://noticias.bol.uol.com.br/internacional/2011/09/09/itamaraty-pede-politica-global-no-combate-a-crimes-ciberneticos.htm

Brasil-MRE & Brasil-MJSP (2019) *Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública* [online]. Available from: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica

Brodie, B. (1959) The Anatomy of Deterrence. *World Politics* [online], 11(02), 173-191.

Buchanan, B. & Rid, T. (2014) Attributing Cyber attacks. *Journal of Strategic Studies* [online], 38(1-2), 4-37.

Bush, G. W. (2002) *The National Security Strategy United States of America*. (September), 1-31. [online]. Available from: http://www.state.gov/documents/organization/63562.pdf

Cançado Trindade, A. A. (2017) *Princípios do Direito Internacional Contemporâneo*. 2nd edition. Vol. 1. Brasília: FUNAG.

Carrel, P. & Rinke, A. (2020) Germany tries to halt U.S. interest in firm working on coronavirus vaccine | Reuters. *Reuters*. [online]. Available from: https://www.reuters.com/article/us-health-coronavirus-germany-usa-idUSKBN2120IV

CISCO (n.d.) *What Is a Cyberattack?* [online]. Available from: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Accessed 11 December 2022).

Colatin, S. (2018) *A surprising turn of events: UN creates two working groups on cyberspace* [online]. Available from: https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/

Council of Europe (2019) Chart of signatures and ratifications of Treaty 185 (Convention on Cyber Crime). Council of Europe [online]. Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Daskal, J. *et al*. (2019) Data and Sovereignty. CyCon US.

Deutsche Welle (2019) Russos protestam contra 'cortina de ferro' na internet. *Deutsche Welle*. [online]. Available from: https://www.dw.com/pt-br/russos-protestam-contra-cortina-de-ferro-na-internet/a-47844381

Elliott, D. (2011) Deterring Strategic Cyberattack. *IEEE Security & Privacy Magazine* [online], 9(5), 36-40.

Ericsson (2020) *Deutsche Telekom and Ericsson strengthen partnership with 5G deal – Ericsson* [online]. Available from: https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal

Fidler, D. (2003) Developments involving SARS, International Law, and Infectious Disease Control at the Fifty-Sixth Meeting of the World Health Assembly | ASIL. *Insights*. 8(14), [online]. Available from: https://asil.org/insights/volume/8/issue/14/developments-involving-sars-international-law-and-infectious-disease

Fidler, D. (2020) *The Cyber Side of Vaccine Nationalism | Council on Foreign Relations* [online]. Available from: https://www.cfr.org/blog/cyber-side-vaccine-nationalism

Fidler, D. (2018) The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers. *Council on Foreign Relations Blog*, 2-5.

Finnemore, M. & Hollis, D. B. (2016) Constructing Norms for Global Cybersecurity. *American Journal of International Law* [online], 110(3), 425-479.

France-Diplomatie (2018) *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace* [online]. Available from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

France-MdA (2019) *International Law Applied to Operations in Cyberspace* [online]. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

GCSC (2019) Advancing Cyberstability. GCSC Final Report.

GCSC (2018) *Norm Package Singapore* (November).

Giles, K. & Monaghan, A. (2014) Legality in Cyberspace: An Adversary View. *The Letort Papers* (March) [online]. Available from: http://www.carlisle.army.mil/ssi

Grigsby, A. (2017) The end of cyber norms. *Survival* [online], 59(6), 109-122.

Grigsby, A. (2018) The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. Council on Foreign Relations, 1-4.

Guterres, A. (2018) *Secretary-General's address at the Opening Ceremony of the Munich Security Conference*. p. 1-6. [online]. Available from: https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general's-address-opening-ceremony-munich-security

Henriksen, A. (2019) The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity* [online], 5(1), 1-9.

Hollis, D. *et al*. (2020) *Elaborating International Law for Cyberspace » directions blog* [online]. Available from: https://directionsblog.eu/elaborating-international-law-for-cyberspace/

Huang, Z. & Mačák, K. (2017) Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. *Chinese Journal of International Law* [online], 16(2), 271-310.

IBM (n.d.) *What is a cyberattack?* [online]. Available from: https://www.ibm.com/topics/cyber-attack (Accessed 11 December 2022).

ICRC (2019) IHL and cyber operations during armed conflicts. UN OEWG/GGE Cyber [online]. Available from: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

Khalip, A. (2018) U.N. chief urges global rules for cyber warfare. *Reuters*, 1-6.

Kharpal, A. (2020) US should take stake in Nokia, Ericsson to counter Huawei in 5G: Barr. *CNBC*.

Korzak, E. (2015a) Have Russia and China signed a Cyber Nonaggression pact? *The Diplomat*, [online]. Available from: http://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/

Korzak, E. (2015b) *The Next Level For Russia- China Cyberspace Cooperation ?* [online]. Available from: https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation

Laudrain, A. (2018) Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace. *Lawfare* [online], 1-2. Available from: https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace

Libicki, M. (2009) *Cyberdeterrence and Cyberwar*.

Libicki, M. (2019) 'Norms and Normalization', in *CyCon US*. 2019 Washington: Army Cyber Institute. p.

Lupovici, A. (2014) The 'Attribution Problem' and the social construction of 'Violence': Taking Cyber deterrence literature a step forward. *International Studies Perspectives* [online], n/a-n/a.

Lynn, W. (2010) Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5).

Mačák, K. (2016) 'Is the international law of cyber security in crisis?', in *8th International Conference on Cyber Conflict* [online]. 2016 Tallinn: NATO/CCDCOE, 127-139.

Malagutti, M. (2016) State-sponsored cyber-offences. *Revista da Escola de Guerra Naval* [online], 22(2), 261-290.

Mearsheimer, J. (2010) The gathering storm: China's challenge to US power in Asia. *The Chinese Journal of International Politics* [online], 3(4), 381-396.

Microsoft (n.d.) *What is a cyberattack?* [online]. Available from: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cyberattack (Accessed 11 December 2022).

Morgan, P. (2010) 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*. 2010 National Academies Press, 55-76.

Morris, L. (2020) Germans to discuss reported U.S. attempt to buy CureVac coronavirus vaccine rights – The Washington Post. *The Washington Post* [online]. Available from: https://www.washingtonpost.com/world/europe/germany-coronavirus-curevac-vaccine-trump-rights/2020/03/15/8d684c68-6702-11ea-b199-3a9799c54512_story.html

Nathan, A. & Scobell, A. (2020) *2020 Data Breach Investigations Report* [online]. Available from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf%0Ahttp://bfy.tw/HJvH

Nederlands-HCSS (2017) *The Global Commission on the Stability of Cyberspace* [online]. Available from: https://www.hcss.nl/news/global-commission-stability-cyberspace

Newman, L. H. (2019) *What Israel's Strike on Hamas Hackers Means For Cyberwar* [online]. Available from: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Nunes, J. (2017) Disease Diplomacy: International Norms and Global Health Security by Sara E. Davies, Adam Kamradt-Scott, and Simon Rushton – Ethics & International Affairs : Ethics & International Affairs. *Ethics & International Affairs* [online], 31(3). Available from: https://www.ethicsandinternationalaffairs.org/2017/disease-diplomacy-international-norms/

Nuttall, C. & Dombey, D. (2009) US urges Twitter to delay service break. *Financial Times* [online]. Available from: https://www.ft.com/content/f317a12e-5acc-11de-8c14-00144feabdc0.

Nye, J. (2018) How Will New Cybersecurity Norms Develop? *Project Syndicate*, 3-5.

Nye, J. (2015) International Norms in Cyberspace. *Project Syndicate*.

Pereira, A. C. A. (2010) A legítima defesa no Direito Internacional contemporâneo. *Revista Interdisciplinar de Direito*, 7(1), 21-36.

Petzinger, J. (2020) Deutsche Telekom describes potential Huawei ban as 'Armageddon' scenario. *MSN* [online]. Available from: https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM

Plening, S. (2009) U.S. State Department speaks to Twitter over Iran. *Reuters* [online]. Available from: https://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616.

Raud, M. (2016) *China and Cyber: Attitudes, Strategies, Organisation*. NATO CCDCOE.

Reilly, J. (2012) A norm-taker or a norm-maker? Chinese aid in Southeast Asia. *Journal of Contemporary China* [online], 21(73), 71-91.

Rid, T. & McBurney, P. (2012) Cyber-Weapons. *The RUSI Journal* [online], 157(1), 6-13.

Rosa, B. & Antunes, C. (2020) Embaixador dos EUA alerta que se Brasil permitir chinesa Huawei no 5G enfrentará 'consequências'. Jornal O Globo. *O Globo*.

Rose, M. & Harvey, J. (2020) France won't ban Huawei, but encouraging 5G telcos to avoid it: report | Reuters. *Reuters* [online]. Available from: https://www.reuters.com/article/us-france-huawei-5g-idUSKBN2460TT.

Roth, A. (2015) Russia and China Sign Cooperation Pacts. *The New York Times* [online], 1-5. Available from: https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html.

Sander, B. (2019) 'The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations', in T Minárik *et al*. (eds.) *CYCON*. 2019 Tallinn: NATO/CCDCOE, 361-381.

Schmitt, M. (2017) *Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations*. NATO/CCDCOE (ed.). Cambridge: Cambridge University Press.

Schmitt, M. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare* [online]. NATO/CCDCOE (ed.), Cambridge University Press.

Schmitt, M. & Vihul, L. (2014) The Nature of International Law Cyber Norms. *CCDCOE Tallinn Papers* [online], 5.

Shackelford, S. (2019) Meet the Coalition Pushing for 'Cyber Peace' Rules. *Defense One*, September.

Sklerov, M. (2010) 'Responding to international cyber attacks', in Jeffrey Carr (ed.) *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly, 46-62.

Stevens, T. (2012) A Cyberwar of ideas? Deterrence and norms in Cyberspace. *Contemporary Security Policy* [online], 33(1), 148-170.

Stoll, C. (1990) *The cuckoo's egg: Tracking a spy through a maze of computer espionage*. The Bodley Head, London.

Toffler, A. (1991) *Powershift: Knowledge, wealth, and violence at the edge of the 21st century*. Bantam Books (Transworld Publishers a division of the Random House Group).

Tuathail, G. Ó. & Agnew, J. (1992) Geopolitics and discourse. Practical geopolitical reasoning in American foreign policy. *Political Geography* [online], 11(2), 190-204.

UN (1945) *Estatuto da Corte Internacional de Justiça* [online]. Available from: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/comite-brasileiro-de-direitos-humanos-e-politica-externa/EstCortIntJust.html

Vital, A. (2008) Tratado sobre crimes digitais sob desconfiança. *Congresso em Foco*.

Wright, J. (2018) Cyber and International Law in the 21st Century. Chatham House.

Zetter, K. (2013) Legal Experts: Stuxnet Attack on Iran Was Illegal "Act of Force". Wired.