TOWARDS A GLOBAL CYBERSECURITY REGIME

DOI: 10.61623/cpe.en.v1n1.a10

Marcel Furtado Garcia[1]

Abstract

The increasing dependence of modern societies on digital networks has heightened their vulnerability to cyber-threats, ranging from human error to state-sponsored malicious attacks. This dissertation examines the potential of a global cybersecurity regime to contribute to international peace and security. Through qualitative research analysing cybersecurity literature, governmental documents, and UN resolutions, it assesses geopolitical challenges stemming from cyberspace, the desirability of a cybersecurity framework to address them, and its feasibility. A global regime could foster stability in the cyber-domain, and, while significant obstacles towards it exist, international efforts suggest progress is possible.

Keywords: Cybersecurity. Balance of Power. International Relations. International Security.

1 First Secretary in the diplomatic service, currently assigned to the Permanent Mission of Brazil to the United Nations in New York. He was deputy chief of the Defense and Cybersecurity Division at Itamaraty between 2023 and 2025. This article was presented as a dissertation in a master's degree course in International Affairs (specializing in cybersecurity) at King's College London.

RUMO A UM REGIME GLOBAL DE SEGURANÇA CIBERNÉTICA

Resumo

A crescente dependência das sociedades modernas em redes digitais vem aumentando a vulnerabilidade às ameaças cibernéticas, que vão desde erros humanos até ataques maliciosos patrocinados pelo Estado. Esta dissertação examina o potencial de um regime global de segurança cibernática que contribua para a paz e a segurança internacionais. Por meio de uma pesquisa qualitativa que analisa a literatura sobre segurança cibernética, documentos governamentais e resoluções da ONU, o trabalho avalia os desafios geopolíticos decorrentes do espaço cibernético, a conveniência de uma estrutura de segurança cibernética para enfrentá-los e sua viabilidade. Um regime global poderia promover a estabilidade no domínio cibernético e, embora existam obstáculos significativos para isso, os esforços internacionais sugerem que o progresso é possível.

Palavras-chave: Cibersegurança. Equilírio de poder. Relações Internacionais. Segurança Internacional.

HACIA UN RÉGIMEN MUNDIAL DE CIBERSEGURIDAD

Resumen

La creciente dependencia de las sociedades modernas de las redes digitales ha aumentado su vulnerabilidad ante las ciberamenazas, que van desde los errores humanos hasta los ataques maliciosos patrocinados por Estados. Esta tesis examina el potencial de un régimen mundial de ciberseguridad para contribuir a la paz y la seguridad internacionales. A través de una investigación cualitativa que analiza la bibliografía sobre ciberseguridad, documentos gubernamentales y resoluciones de las Naciones Unidas, evalúa los retos geopolíticos derivados del ciberespacio, la conveniencia de un marco de ciberseguridad para abordarlos y su viabilidad. Un régimen global podría fomentar la estabilidad en el ciberespacio y, aunque existen obstáculos importantes para su consecución, los esfuerzos internacionales sugieren que es posible avanzar.

Palabras clave: Ciberseguridad. Equilibrio de poder. Relaciones internacionales. Seguridad internacional.

Introduction

The digital transformation of modern societies has been a driver of development and well-being. At the same time, societies have become increasingly contingent upon the constant and correct functioning of digital information network systems, much as they largely depend on, for instance, the availability of electricity. This dependency entails vulnerabilities to inherited flaws, human errors, accidents or malicious actions that may adversely affect those systems.

This vulnerability is not new. Throughout history, information systems have presented challenges. Long before electronic networks emerged, advances in communication technology had been exploited by "hackers." As early as 1834, criminals breached the French telegraph system to transmit hidden information about and profit from the national financial market (Standage and Stevenson 2018). The birth of cyberspace occurred 135 years later, with the first computer connection established between the University of California and Stanford University (Singer and Friedman 2014, 16–18). By the early 1970s, efforts were already being made to address vulnerabilities in electronic systems (U.S. Cyber Command 2024). The first cyberattack with significant physical consequences may have occurred in 1982, when the Urengoy-Surgut-Chelyabinsk pipeline in Russia exploded, allegedly due to software sabotage by the CIA (Rid 2013, 4–5). A new source and means of international conflict and power was emerging.

The world was recently reminded of the extent of today's cyber-vulnerability. In mid-July 2024, chaos ensued after human error disabled digital systems across the world, including essential services such as banking, healthcare and air travel (Plummer and Gerken, 2024). This resulted from failures in cloud-based security software updates by CrowdStrike, which is used by Microsoft's main platforms. While this event was unintended, it was perhaps the latest large-scale warning of the potential scope and reach of harm an offensive cyber-operation could achieve, worldwide and with immediate effects, especially when carried out with geopolitical goals.

Research question

This warning renewed the call to address this new, global and digital avenue for malicious actions. In this context, this dissertation will focus on interstate conflict in cyberspace and ways to avoid it and uphold stability, under the main question "to what extent could a global cybersecurity regime

contribute to international peace and security?" As will be seen next, the main question will be supported by two secondary ones, the first related to the context in which it is found, and the second related to the feasibility of such a regime.

Approach and structure

This dissertation is based on qualitative research focussed both on cybersecurity literature and analysis of primary sources, including government documents, official speeches in multilateral fora, and United Nations resolutions and reports. Combined, these materials provide a broad theoretical and empirical basis for assessing the challenges and developments relating to an international framework of responsible state behaviour in cyberspace and the prospects of a global security regime for this dimension, aimed at mitigating threats to international peace and security.

Following this introduction, three Chapters will discuss the different aspects involved with such a prospect. Chapter 1, "Cybersecurity challenges," will provide the background for answering the main question. First, it will assess the international strategic landscape derived from the nature of cyberspace, in particular how it affects states' power and geopolitical rivalry, becoming a source of international instability. Second, with a view to exploring systemic ways to mitigate cybersecurity challenges, the Chapter will review liberal institutionalist assumptions and assessments of international regimes, as frameworks of incentives that may mitigate threats to peace and security. These incentives are not seen as unequivocal or inevitable but may be effective in avoiding violent interstate conflict.

Chapter 2, "Desirability of a regime," will most directly address the main question. It will first cover domestic options to address cyber-threats and their likely international consequences. It will then contrast these with the possible contributions from a global cybersecurity regime, arguing that the latter provides preferable incentives, despite its limitations. In particular, the definition and clarification of norms of state behaviour in cyberspace, if broadly shared, would diminish ambiguities and avoid misperceptions. By combining this with global efforts towards cyber-resilience through capacity-building, a regime could provide strong enough influence to alter cost-benefit perceptions, discouraging state-sponsored malicious cyber-operations and favouring stability in the digital dimension.

However, a global cybersecurity regime would confront important limitations. If a global cybersecurity regime is to contribute to international

peace and security, it is necessary to assess how attainable and effective it would be. In addition to the challenges faced by regimes in general, a cybersecurity one would encounter new layers of difficulties for its establishment and running, both technical and political. These will be explored in Chapter 3, "Feasibility of a regime." This Chapter will argue that, despite their magnitude, they are not insurmountable, and have been addressed, with some degree of success, by the international community. While the emergence of a global cybersecurity regime is not inevitable and will further demand significant efforts, the UN General Assembly (UNGA) has already taken important steps in that direction.

1. Cybersecurity challenges

This Chapter will first introduce the international challenges derived from cyberspace and then provide a review of the liberal institutionalist's perspective on regime theory. It will outline the theoretical framework for the following ones, providing the background to assess this dissertation's main question.

International security and cyberspace

This section will briefly review the nature of cyberspace, as it differs from the "traditional" domains of geopolitical rivalry, and how it affects international security. To that end, it will provide a definition and context of cyberspace and cyberpower, and evaluate how these affect the international security environment.

Definition and context

For the purpose of this work, cyberspace will be understood as the man-made virtual domain formed by three mutually dependent layers: physical (hardware and associated infrastructure); logical (data, software and protocols); and cognitive/social (related to interaction of human users). This dissertation will use the term 'cyberspace' as a synonym for 'information and communication technology (ICT) environment.'

As all human systems (finance, communication, military and so on) come to be dependent on the constant availability of digital infrastructure and software, malicious cyber-operations could, in principle, disrupt any cyber-system anywhere. In this sense, a "laptop can produce global consequences" (Kissinger 2014, 345). While the CrowdStrike incident mentioned in the

Introduction was unintended, several others have demonstrated the capacity of malicious cyber-operations to inflict significant harm, including with political goals.

Two milestones are particularly illustrative. At the end of 2009, the malware "Stuxnet" affected the centrifuges in the Iranian nuclear enrichment plant in Natanz and imposed a severe setback on the country's nuclear programme (Kello 2013, 19–20). In late April 2022, Costa Rica became the first country to declare a state of emergency following massive cyberattacks that disabled several essential national services. The attackers called for the overthrow of the federal government (Burgess 2022). These and other cyber-incidents have demonstrated that cyberspace has become a dimension of international conflict (Clarke and Knake 2010, 6–30).

The possibilities of malicious actions in or from cyberspace, across and through its multiple layers, have opened unprecedented avenues for the conduct of interstate geopolitical rivalry. This is a direct result from the dimension's main characteristics: anonymity and opacity (and consequent deniability of operations); intangibility of capabilities; virtual suppression of distances and time; and global reach (Betz and Stevens 2011, 9–10). Cyberspace provides a set of possibilities for hostile actions, including espionage, monitoring, subversion, disruption and sabotage (Belk and Noyes 2012, 5).

Different scholars consider states' cyber-capabilities as "strategic levers," given their capacity to heighten conventional instruments of power (Nye 2011, 123; Sheldon 2011, 104; Kissinger, Schmidt and Huttenlocher 2021, 150). Such capabilities become, themselves, resources of power (Nye 2011, 123), which can be instrumentalized to manipulate the security environment and produce "preferred outcomes" within or outside cyberspace (Nye 2014, 5).

Security environment

Geopolitical rivalries have been shifting from the kinetic to the virtual dimension (Kissinger 2014, 347), and states have recognised that cyber-tools can threaten their security. NATO's 2022 Strategic Concept affirms that "[c]yberspace is contested at all times" (NATO 2022, 5) potentially leading Alliance members to invoke Article 5 of NATO's Treaty (ibid., 7). The UN member-states have expressed concern regarding the development of cyber-capabilities "for military purposes" and their possible use in future conflicts, acknowledging that threats stemming from cyberspace can be a source of international volatility (United Nations General Assembly, A/RES/75/240, 2020). The latter derives from the defence and offence challenges that cyberspace engenders, which alter states' strategic calculations.

Defence challenges

Defence premises against cyberattacks differ sharply from those against kinetic ones. Offensive cyber-operations are unpredictable, and the defender may be unaware of vulnerabilities that could be exploited by intangible and unknown cyber-capabilities of rivals (Kello 2017, 68–69). There is a high degree of uncertainty regarding the identity of the attacker (ibid., 129–130). Finally, cyber-conflict is marked by a crucial paradigm shift, from territorial defence against invasion, to the assumption that the cyber-enemy is already in, undetected (ibid., 6).

Another central challenge concerns the threshold problem. There is a lack of reference of when a cyber-attack would equate a kinetic one. Attackers may thus engage in a series of low-level cyber-aggressions, testing a defender's reactions and reaping benefits while trying to avoid triggering a major response (Mazarr 2018, 10; Kello 2022, 13).

Offence challenges

In this scenario, some states have established policies of "preemptive attack." The USA, for example, acknowledges that it has been "actively disrupting malicious cyber-activity before it can affect the U.S. Homeland" (United States of America 2023, 1). Preemptive attacks may also seek to guarantee that, in a future situation of open hostility, a state will be able to penetrate and disrupt a rival's digital systems (Andres 2012, 94–95).

Such policies, however, widen the scope for mistakes, accidents, and inadvertent escalation, while fast or automatic digital reactions and counter-reactions may decrease de-escalation opportunities (Eilstrup-Sangiovanni 2018, 387). Furthermore, malicious cyber-activities aimed at future disruption of a digital system may promptly disable it, and malwares could spread further than originally planned (Andres 2012, 94–95). These preemptive policies also contribute to a larger scenario of systemic volatility, as they circumvent international law, which disciplines and limits the use of force to very specific cases.[2]

Strategic landscape

These challenges engender significant problems for strategic assessments and balance of power dynamics. If a nation's power could once be assessed by a combination of factors such as population, economic robustness and

2 See, for instance, Arts. 2.4 and 51 of the UN Charter.

military equipment (Kissinger 2014, 344), relative power calculations today are complicated by the opacity of cyber-capabilities (Eilstrup-Sangiovanni 2018, 390). As Kissinger, Schmidt, and Huttenlocher warn, "[w]hen the calculation of equilibrium becomes uncertain, or when nations arrive at fundamentally different calculations of relative power, the risk of conflict through miscalculation reaches its height" Kissinger, Schmidt and Huttenlocher 2021, 151).

This volatility is accompanied by the blurring of the frontier between war and peace in cyberspace. Kello has coined the term "unpeace" to characterise this state of affairs. He defines it as a "mid-spectrum rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition and possibly, even, of war" (Kello 2017, 78).

While cyberspace becomes "strategically indispensable" (Kissinger 2014, 346), there is a severe lack of common understanding not only regarding the "rules of the game" of cyber-rivalry (Hurwitz 2013-2014, 21–22), but, more importantly, of the changing international security landscape itself (Kissinger 2014, 344). This scenario deprives states of the common assumptions and references necessary to conduct restrained conflict (Kello 2013, 31).

How to tackle this new reality? Regime theory argues, among other points, that states may, through international institutions, succeed in reducing uncertainty and perceptions of vulnerability. The academic literature on this will be addressed in the next part of this Chapter.

Regime theory

Advocates of international regimes argue that states may mutually benefit from institutions. This dissertation will apply this argument to cyberspace in order to assess the extent to which a global regime could address the challenges that emerge from this new dimension of interstate rivalry.

To that end, this section will briefly (1) explain the theoretical focus of this dissertation; (2) review the main literature on international regimes; and (3) introduce the application of regime theory assumptions to cyberspace, which will be further explored in the next Chapters.

Theoretical focus

States. While non-state actors may also employ cyber-tools to inflict considerable harm in and from the cyber-dimension, this dissertation will focus on states, which are (still) the main actors in the international security framework, including in cyberspace (Goodman, 2010, p. 105).

Liberal institutionalism. Regime theory assumes that interstate conflict is not inevitable. This view is best developed by the liberal institutionalism school of International Relations (IR), which will be applied in this work. An alternative approach would be to adopt the constructivist perspective of norm formation and influence on state behaviour (Fazal, 2024). However, the development of the so-called "norms of responsible state behaviour in cyberspace"[3] derives from states' negotiations and focuses on threats to states' material capabilities, especially critical infrastructure. Moreover, the opaque nature of cyberspace adds an extra layer of difficulty in observing the formation of norms through social interaction, as well as how they may actually affect state behaviour (Checkel 1998, 340). Although such difficulties also impose challenges on liberal institutionalism's perspective on regime formation, the choice to adopt this approach derives from the fertile material provided by the UNGA discussions of those very norms and of a future permanent, universal mechanism dedicated to cybersecurity.

"Global" cybersecurity regime. The word "global" was chosen to stress universality in terms of the membership and reach of such a regime, as opposed to more limited ones that are also international (e.g., regional, cross-regional etc.). Crucially, this indicates the necessity of having rival states interacting under mutually agreed rules and procedures.

Liberal institutionalism and critics

Krasner defines regimes as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations" (Krasner 1982, 186). For Keohane, states follow such principles, norms, rules and procedures, abdicating part of their freedom of action, because they expect to obtain mutual gains, even in the absence of a higher authority to oversee or guarantee compliance to the regime (Keohane 1982, 332). Regimes are beneficial because they provide a framework to reduce transaction costs, creating "a more favourable institutional environment for cooperation than would otherwise exist," thus facilitating negotiations and legitimising state actions (Krasner 1982, 334–338; Keohane 1984, 244; Nye 2014, 5). According to Nye, states already obtain benefits from existing norms in the digital realm, which, for instance, underpins the functioning of the internet (Nye 2014, 5–7).

Liberal institutionalism's view of regimes is far from consensual. Susan Strange asserts that international regimes tend to serve as "instruments of

3 Officially adopted through UNGA Resolution 71/28 (December 2016).

the structural strategy and foreign policy of the dominant state or states" (Strange 1982, 484), in such a way that the regime lenses are "biased toward the status quo" (ibid., 488). In the same vein, Mearsheimer affirms that powerful states may support regime building, but only to maintain or increase their own power (Mearsheimer 1994-1995, 13). Moreover, he highlights the uncertainty derived from the possibility of cheating at the established rules and norms (ibid.).

Even advocates of regimes recognize limits and challenges faced by international regimes. Keohane points, for instance, to their comparative fragility when compared to domestic rules and norms. This is due to the decentralised, anarchic and self-help nature of the international system (Keohane 1984, 62). While this recognition converges with some of the arguments raised by critics of regimes, liberal institutionalists stress that regime theory does not disregard "power and interests," nor intend to "constitute a panacea for violent conflict." It rather aims at shedding light on when and how regimes may impact state behaviour (Keohane and Martin 1995, 50). An example is through the provision of high-quality information that would, among other things, reduce uncertainty by discouraging cheating and mutual distrust (ibid., 49).

Regimes and international peace and security

Regimes could contribute to the stability of the international system by, for example, preventing the so-called "security dilemma," a dynamic circumstance in which a nation's security improvement is perceived as a menace by a rival. This perception of vulnerability derives from uncertainty regarding a state's intentions vis-à-vis others under an anarchic system.

A situation of security dilemma may result in an arms race and uncontrolled escalation (Jervis 1978, 169–170). Jervis warns that "unrestrained competition can harm all the actors," as "individualistic actions are not only costly but dangerous" (Jervis 1982, 358). Cyberspace is prone to the same risks. Kissinger alerts against the "self-defeating nature of unconstrained national conduct" in this realm (Kissinger, 2014, p. 346). To him, "absent some articulation of limits and agreement on mutual rules of restraint, a crisis situation is likely to arise, even unintentionally" (ibid.).

The establishment of any regime, however, is a complex endeavour. Jervis has examined these difficulties in the security field, compounded by the security dilemma. In his view, this makes international security regimes both desirable (given the risks of individual actions and resulting reactions) and

difficult (once "the fear that the other is violating or will violate the common understanding is a potent incentive for each state to strike out on its own even if it would prefer the regime to prosper") (Jervis 1982, 358). The next Chapters will address these features (desirability and difficulty) related to a possible cybersecurity regime.

Partial conclusion

This Chapter defined and contextualized cyberspace as a domain of interstate rivalry, prone to unprecedented volatile dynamics that may result in risks to international peace and security. While cyber-attacks have demonstrated how harmful they may be, there is a lack of standards for states to assess both the alteration of the strategic environment and of the rules of the game of the cyber-rivalry.

In turn, liberal institutionalists have pointed out how regimes may be of mutual benefit for states, preventing security dilemma dynamics, by, for example, establishing norms and promoting convergence of expected behaviour. To these scholars, while security regimes are not a panacea, they do support stability and may avoid violent international conflict.

The next Chapters will apply this view to the cyber-dimension. Following Jervis' assessment of security regimes as being desirable and difficult, they will assess the desirability (Chapter 2) and feasibility (Chapter 3) of establishing a global cybersecurity one.

2. Desirability of a regime

This Chapter will be divided into two sections. First, it will touch upon the main domestic approaches against cyber-threats and their impacts on international security. Second, it will assess how a global regime could contribute to international cybersecurity, pointing to what would constitute its central pillars. This second section will argue that a global regime could successfully increase systemic cybersecurity, while avoiding the shortcomings of offensive options. It will also consider some limitations of such a regime.

Domestic approaches

Scholars point to different options to address cyber-threats to international peace and security. While some domestic policies and strategies may tackle such threats, some of them may incite distrust and rivalry in and through cyberspace, being themselves a source of systemic instability.

Assessing the challenges imposed by state-sponsored hostile cyber-operations below the threshold of war, Kello affirms that possible solutions "must be found not primarily in current law and norms, but in … figuring out how to respond to activity – in order to deter its recurrence" (Kello 2022, 16). He argues that the current international framework of norms has failed to hinder state rivalry in cyberspace, and urges Western countries to develop a "new doctrine" that would avoid placing "the international order at the mercy of the players most eager to defy it" (ibid., 25).

This view converges with arguments supporting the strengthening of cyber-deterrence, especially with unilateral retaliatory policies (or "deterrence-by-punishment"). NATO, for example, has such a policy in place encompassing, and potentially crossing, all strategic dimensions, including cyberspace (NATO 2022, 6). However, deterrence-by-punishment involves significant challenges, including the need for a state to have the capability and the will to retaliate against aggressors (Mazarr 2018, 10). This approach is particularly complicated by the opaque nature of cyber-operations and the resulting difficulties of uncovering the perpetrators behind them. Even Kello admits that the attribution problem "weakens deterrence by reducing an assailant's expectation of unacceptable penalties" (Kello 2013, 33). Moreover, deterrence-by-punishment policies may fuel geopolitical rivalry and engender escalatory dynamics, given the blurred boundaries between defensive and offensive operations, the lack of clarity regarding what would constitute a proportionate retaliation, and the determination of some countries to punish across domains (NATO 2022, 6). As Mazarr warns, "threat-based deterrence strategies can go tragically wrong and provoke the very conflicts they are meant to avoid" (Mazarr 2018, 5).

In turn, "deterrence-by-denial" differs deeply from its retaliatory cousin. As seen, cyberattacks tend to be unpredictable and undetectable. As Stuxnet has shown, a malware might find its way into a digital system regardless of its defences and isolation (Clarke and Knake 2010, 292; Kello 2017, 197–198). This is not to say that deterrence-by-denial has no value. Stuxnet has also demonstrated that infecting a complex and well-defended system requires a level of resources available only to a limited number of international actors. Denial policies aiming at increasing the futility rate of possible attacks are thus valuable (Goodman 2010, 106). They are directly related to the system's resilience and hinge upon the availability of defence resources, including human skills, of the potential victim (Nye 2016-2017, 56–57). Despite being imperfect and uncertain, denial policies avoid the systemic shortcomings derived from offensive approaches, including "preemptive" ones (Chapter 1). On the contrary, the former entail systemic benefits, given that cyberattacks

may have cross-border ramifications (Kello 2017, 6). For that reason, denial policies a key element in a global cybersecurity regime.

As Nye underlines, in isolation, these domestic approaches can only have limited results. To be effective, they would need to be complemented with an international multi-layered framework aimed at deterring malicious cyber-actions (Nye 2016-2017, 62). In this vein, the next section will assess the most important of these layers, which would constitute the main pillars of a global cybersecurity regime.

Contributions of a global regime

Other scholars coincide with Nye in that a multi-layered, international framework of policies and strategies could effectively counter systemic threats to peace and security stemming from cyberspace (Goodman 2010, 109; Mazarr 2018, 11). Likewise, this dissertation will argue that the combination of global norms, capacity-building policies, and the resulting alteration of cost-benefit perceptions of malicious cyber-operations could create an architecture of incentives influential enough to shape states' behaviour and uphold stability in cyberspace.

Global norms

The establishment of a global cybersecurity regime, as defined by Krasner (Chapter 1), would require states to agree on the "rules of the game" around which expectations converge.

The drawing of clear lines of state behaviour would allow for restrained geopolitical rivalry in the digital domain (Eilstrup-Sangiovanni 2018, 383–384), avoiding, for example, unilateral policies that risk attracting "chaos in determining an appropriate response to cyberattacks," or drawing "adversaries to test the waters" by engaging in offensive operations below the threshold of war (Pratick 2018).

Crucially, the systemic threats stemming from the nature of cyberspace call for a global effort towards establishing rules of the game that are broadly shared. While restricted international initiatives may be valuable to raise awareness and initiate discussions on specific complex issues, they lack, by definition, universality and present an inherent legitimacy gap. They risk alienating major players and fuelling existing geopolitical rivalry and distrust. A recent example is the so-called "Pall Mall Process," focused on "tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities" (United Kingdom 2024). According to the joint declaration approved in its

first meeting, Pall Mall partners would "engage in an ongoing and globally inclusive dialogue, complementary to other multilateral initiatives." This remains to be seen, as the list of participants is mostly formed by developed Western states and non-governmental entities.

Conversely, efforts towards establishing cybersecurity norms should aim at minimizing ambiguity globally, if they are to reduce risks of misperceptions and miscalculations (Hurwitz 2013-2014, 20–21). The international community has taken important steps in this direction. In 2015, the UNGA endorsed a framework of "Norms, rules and principles for the responsible behaviour of States" (United Nations General Assembly, A/70/174, 2015) and, in 2021, those norms were further developed (United Nations General Assembly, A/76/135, 2021). Though non-binding, the framework was endorsed by consensus,[4] conferring on it significant political weight.

Despite this achievement, there is still much to be done regarding ambiguity in cyberspace. There is a fundamental lack of common understanding even related to how international binding rules already in force apply in this realm. Some countries have been publishing unilateral positions on this issue, but national perspectives are still very broad and vague. The USA, for example, has affirmed that the right to self-defence may be triggered "by cyber activities that amount to an … armed attack," with no reference on how to arrive at that conclusion (United Nations General Assembly, A/76/136, 2021, 137). In this context, Brazil has recommended the "update [of] the multilateral understanding of which acts amount to the use of force and aggression, so as to include instances of cyberattacks" (ibid., 19).

A central ambiguity relates to the relationship between the principle of sovereignty and the layered and cross-border nature of cyberspace. For Israel, while "States occasionally do conduct cyber activities that transit through, and target, networks and computers located in other States … [u]nder international law, it is not clear whether these types of actions are violations of the rule of territorial sovereignty" (Schöndorf 2021, 403).

The controversy goes further. States differ in their understanding regarding the concept of sovereignty itself in relation to cyberspace. This issue divides even NATO allies. For the United Kingdom, "the general concept of sovereignty by itself [does not provide] a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention" (United Nations General Assembly, A/76/136, 2021, 117).

4 The documents were endorsed by UNGA Resolutions 70/237 and 76/19, respectively.

In turn, Canada considers that "[i]t is axiomatic that the principle of sovereignty applies in cyberspace, just as it does elsewhere" (Canada 2024).

Arguably, if states are to avoid misperceptions, miscalculations and volatility in cyberspace, there is a need to consider common grounds and establish global norms for their operations, especially regarding those basic concepts and principles that have underpinned interstate relations at least since the Westphalian treaties. The international community has, at least since 2010, recognized that "the absence of common understanding regarding acceptable State behaviour may create the risk of instability and mispercept on" (United Nations General Assembly, A/65/10, 2021, para. 7).

Capacity-building

Capacity-building is key for national as well as overall cyber-resilience. "Capacity" in this context relates to having institutional maturity, as well as availability of appropriate national resources, including a skilled workforce, to prepare against and respond to cyber-incidents (Hurel 2022, 70). National capacity directly influences collective cybersecurity, given the possible cross-border nature of incidents, in particular risks to transnational supply-chains. The mid-2024 CrowdStrike incident (Introduction) is evidence of such global risks.

The international community recognizes the importance of capacity-building for cybersecurity. The ongoing Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies, tasked by the UNGA to address cybersecurity challenges (United Nations General Assembly, A/RES/75/240, 2020, para. 1), has recently reaffirmed that capacity-building is transversal to different cyberspace challenges and contributes to building a secure and peaceful cyberdimension (United Nations General Assembly, A/79/214, 2024, 6).

Some regional initiatives are illustrative of international efforts to promote capacity-building and collective resilience. "CSIRTAmericas," of the Organization of American States (OAS), offers its members a platform for exchange of information, technical assistance and training for specialists, helping countries to improve their institutional preparedness against cyber-threats (Organization of American States 2024). The "ASEAN-Singapore Cybersecurity Centre of Excellence" (ASCCE) conducts research and training activities, facilitating communication and sharing of experience and cyber-threat related information and best practices (Cyber Security Agency of Singapore 2021).

Regional experiences could inspire a multilateral resilience mechanism. Some steps have already been taken in that direction. The OEWG approved, in 2023, principles to guide international capacity-building activities (United Nations General Assembly, A/78/265, 2023, annex C). In May 2024, it convened a first global high-level meeting on capacity-building at the UN Headquarters. Different stakeholders had an opportunity to share views on ways to mobilize and optimise the use of resources for sustainable international capacity-building action (United Nations Institute for Disarmament Research 2024, 17). Finally, in 2022, a "Global Intergovernmental Points of Contact Directory on the Use of ICTs in the Context of International Security" was established by the UNGA (United Nations Office for Disarmament Affairs 2024). The Directory aims to facilitate interstate coordination and communication, and to provide a platform for future activities, including capacity-building ones. The Directory could become a first institutional step towards a mechanism focussed on harnessing, fomenting and giving coherence among different international capacity-building actions. Fundamentally, these developments show how international institutions may facilitate interstate negotiations and cooperation, as stressed by Keohane (Chapter 1).

Along with the establishment of universal cyber-norms, global capacity-building efforts could help reduce expected gains from malicious operations, while increasing their costs. This alteration of cost-benefit perception is the third pillar of an effective global cybersecurity regime.

Cost-benefit perceptions

As recognised by some states (United States of America 2023, 2) and scholars (Nye 2016-2017, 53; Eilstrup-Sangiovanni, 2018, p. 387; Goodman 2010, 107–108), perceptions influence cost-benefit calculus and behaviour in cyberspace. This is a key psychological aspect influenced by international regimes (Chapter 1). Derived from the establishment of norms and capacity-building efforts, a successful global cybersecurity regime would alter cost-benefit perceptions in at least two ways.

First, establishing clear, global and legitimate norms and rules on what is unacceptable, on how to identify transgressors, and on when and how to respond collectively to aggressors would significantly increase the cost of cheating. The definition of thresholds could protect certain critical systems and create taboos (Nye 2016-2017, 60–61). In turn, the institutionalization of procedures to collectively identify transgressors and respond to malicious operations could discourage unilateral retaliation, including offensive actions

that may be deemed illegitimate, disproportionate or against the wrong target (as in cases of misattribution). On the contrary, a regime would channel major violations to the established multilateral bodies that hold the legitimacy to address them in the name of the international community. The International Atomic Energy Agency (IAEA) statute, for instance, determines, among other measures, that non-compliance or issues of particular gravity be brought to the attention of the UN Security Council and General Assembly (International Atomic Energy Agency, 1956, art. XII.c).

A clear and broadly accepted framework of cyber-norms would support international law in general, including self-defence rules enshrined in the UN Charter (Articles 2.4 and 51). This could have a reinforcing effect on the cyber-norms framework itself, strengthening incentives against malicious actions in and from cyberspace. Potential cyber-aggressors could be discouraged, along with the perception of vulnerability, which lies at the heart of security concerns, including security dilemma dynamics (Chapter 1).

Second, a regime could support official mechanisms of international cooperation aimed at assisting countries in preparing for and responding to malicious cyber-operations. This would also reinforce national deterrence-by-denial policies, by increasing the futility of possible aggressions (Nye 2016-2017, 56). This support could also favour the sustainability of the digital transformation in countries, which hinges upon the availability and correct functioning of digital systems. This is essential not only for their human development, but also for systemic resilience. As a recent report of the World Economic Forum pointed out, digital inequity is a "driver of ecosystem risk," given that "the overall resilience of the ecosystem is often determined by its weakest links" (World Economic Forum 2025, 29). Therefore, cost-benefit perceptions, from a systemic perspective, would depend on elevating collective resilience.

Limitations

Naturally, a global cybersecurity regime would face considerable limitations and challenges.

First, realists' claims that regimes are contingent on the international power structure (Chapter 1) should be kept in mind. An example is the ousting of the first director-general of the Organisation for the Prohibition of Chemical Weapons, José Bustani, less than two years after he was unanimously reappointed to that position, and a year before the 2003 invasion of Iraq (Stanič 2004, 814). Bustani was considered one of the "key obstacles to the

war because [he was] proposing nonviolent methods of eliminating Saddam's alleged stockpiles of such weapons" (Stanič 2004, 810). This case recalls Strange's warning that regimes are partial towards the status quo, showing how their internal processes may be compelled to guarantee it.

Second, there are specific and significant challenges related to the establishment and the running of a global cybersecurity regime. These will be explored in the next Chapter.

Partial conclusion

Realists point to important limitations of international regimes. The Bustani case is an important reminder that regimes should be perfected constantly, including with a view to mitigating, as much as possible, interference from power politics and geopolitical circumstances.

Conversely, as liberal institutionalists have pointed out, regimes are not conceived to be a panacea. This Chapter has attempted to demonstrate that, since cyberspace is prone to volatile dynamics that may threaten international peace and security, there is value in pursuing a global cybersecurity regime.

Domestic options may not only be insufficient to address cyber-threats, but may instead fuel interstate rivalry and international instability, as in the case of preemptive and retaliation-based policies. In turn, a global regime combining universal norms and capacity-building efforts could be influential enough to alter cost-benefit perceptions and discourage interstate rivalry through malicious cyber-operations.

A global cybersecurity regime could significantly contribute to international peace and security and is therefore desirable. The establishment of the norms of responsible state behaviour and the steps taken by the UNGA to foster international capacity-building efforts are therefore to be welcomed. However, the possible establishment and running of a global regime would certainly face fundamental limitations and challenges. The next Chapter will focus on these.

3. Feasibility of a regime

If a global cybersecurity regime is desirable, it is necessary to address the specific challenges involved in its establishment and running. This Chapter assesses the main technological and political ones. Although they are significant, this dissertation will argue that they are not insurmountable.

The Chapter will end by reporting on recent experience that demonstrates the international community's current engagement in this task.

Regime challenges

As Jervis highlights (Chapter 1), the establishment of security regimes is a complex and uncertain endeavour. The nature of cyberspace adds further challenges, both technical and political.

Technical challenges

The main technical challenges for a cybersecurity regime arise from the ubiquity and intangibility of cyberspace. These characteristics result in critical difficulties in defining thresholds for malicious operations, establishing verification mechanisms that would investigate and attribute attack, and inducing compliance with the norms of a regime.

Threshold. As seen (Chapter 2), there is significant ambiguity related to the rules of the game in cyberspace, including when cyber-operations may reach the level of an armed attack. The latter is particularly important, because it is a necessary condition to trigger international responsibility and the right to self-defence. So far, the international community has only been able to provide general norms of responsible behaviour, including that a state should not damage critical infrastructure through cyber-operations.[5]

Verification. Several security regimes have established verification mechanisms in order to increase mutual trust and discourage cheating. A major challenge they face is the dual-use of the material that falls under their purview. In 2023, for instance, the IAEA applied safeguards in 189 states in order to ensure they are using dual-use nuclear material in accordance with their international legal obligations (International Atomic Energy Agency 2024). It seems, however, improbable that techniques and expertise developed by the existing security regimes to verify compliance could provide guidance for a cybersecurity regime. The weaponization of software, which are not only dual-use, but also intangible (Nye 2018, 336), would seem to pose an apparently insurmountable technical challenge for the establishment of such a mechanism that would discourage cheating (Nye 2016-2017, 50).

Attribution. A related challenge is finding the culprit behind cyberattacks. Several features render cyber-attribution particularly problematic, including the considerable degree of anonymity; the difficulty of identifying the human

5 Norm "f" of the norms of responsible state behaviour.

actor, even having found the IP address of the machine used in the attack; and the ease with which malwares cross jurisdictions (Kello 2013, 33).

States investigating cyberattacks employ undisclosed cyber-capabilities and intelligence apparatus, and seldom provide substantial evidence of their findings. This makes attribution "an inherently political act" (Egloff 2019, 55). Some scholars have noted important bias tendencies behind attribution policies, due to geopolitical interests (Hurel 2022, 79) and to commercial goals (Oosthoek and Doerr 2021, 309). This leads to lack of legitimacy and to contestation of attribution and of retaliation based thereon. Moreover, the possibility of misattribution may be exploited by malicious actors (Hurwitz 2013-2014, 20).

States have recognized these challenges. The framework of responsible state behaviour in cyberspace underlines that "accusations of organizing and implementing wrongful acts brought against states should be substantiated" (United Nations General Assembly, A/76/135, 2021, 18). Moreover, international customary law defines that an internationally wrongful act of a state consists of an action or omission that is attributable to the state under international law (International Law Commission, 2001, art. 2.a). An accurate attribution against a state would therefore require the correct identification of an IP address and of the operator, as well as his/her connection with the accused government (ibid.; Rid 2013, 144–145; Schmitt and Vihul 2015, 45).

Political challenges

The main political challenge is probably states' unwillingness to restrict their own behaviour. This reluctance derives particularly from the relative novelty of cyber-operations as power levers and the secrecy behind states' cyber-capabilities. As Schmitt and Vihul stress, "states are hesitant to restrict the use of [cyber]weapons that may afford them an advantage on the battlefield until they have sufficient experience to allow them to weigh the costs and benefits of prohibitions and limitations on their use" (Schmitt and Vihul 2015, 45). Furthermore, while much of the impact of cyber-capabilities derives from their concealed nature (Kissinger 2014, 347), any international restriction would require agreement on some degree of definition related to what is to be restricted.

There are no prospects of global negotiations regarding such restrictions, as states are divided on this issue (Singer and Friedman 2014, 185–186). While Russia has presented a blueprint for a global cybersecurity treaty (Russian Federation 2021), several Western countries affirm either that there

is no need for a new international binding instrument, or that several steps should be taken before considering the possibility (European Union 2023).

Parallels could be drawn between this scenario and the development of the international nuclear regime, which started to take shape after the most advanced countries felt certain of their technological superiority and only then assumed a leadership role to prevent uncontrolled proliferation (Eilstrup-Sangiovanni 2018, 404–405). As the race for the development of the most advanced cyber-capabilities is still ongoing, the current discussions on cyber-norms are still subordinated to the international power rivalry, "rather than a unified search for normative order, clarity, and predictability" (Tikk 2021, 751).

Addressing the challenges identified

An emerging cybersecurity regime would need to face cyber-specific technological and political challenges, to which there is not much precedent to serve as a guide. As Andres stresses, "[i]n the case of cyber threats, the past is not necessarily prologue" (Andres 2012, 90). Moreover, the fast pace of technological development will probably continue to pose unprecedented difficulties, the reason why "laws and regulations are always chasing a moving target" (Nye 2014, 6). Nevertheless, as will be seen next, there are ways to address the current challenges, and the international community already seems to be making important progress in that direction.

Addressing the technical challenges

Threshold

Internationally accepted definitions in the security area may take a considerable time to emerge. For instance, "act of aggression," mentioned in Chapter VII of the UN Charter, was defined almost three decades after the instrument came into force (United Nations General Assembly, A/RES/3314(XXIX), 1974).

In turn, the UNGA has already defined certain boundaries that states should not cross in cyberspace. For example, Norm "f" of the norms of responsible state behaviour affirms that a "State should not conduct or knowingly support ICT activity … that intentionally damages critical infrastructure…" Norm "i" establishes that "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."

The important nuance between Norm "f," which uses negative and prohibition language, and Norm "i," which encourages certain steps to be taken, indicates different degrees of concern within the international community that could lead to further common understandings of where threshold or red lines should be drawn.

Verification and attribution

As cyber-technology is inherently dual-use and intangible, multilateral verification activities would probably need to focus on malicious actions, instead of on capabilities, providing for an *ex post-facto* monitoring. As suggested by Eilstrup-Sangiovanni, the International Monitoring System of the Comprehensive Nuclear-Test-Ban Treaty (CTBT) may be a source of inspiration (Eilstrup-Sangiovanni 2018, 395). Despite the fact that the CTBT has not entered into force, its Preparatory Committee (CTBTO-PrepCom) has managed to put in place an impressive system with proven efficiency, having quickly and accurately identified North Korea's nuclear explosion tests (Comprehensive Nuclear-Test-Ban Treaty Organization 2024).

Experience in combating cybercrimes has demonstrated that attribution may not be "the insurmountable challenge that theoretical models suggest" (Goodman 2010, 105). Law enforcement has demonstrated that forensics is essential to curb cybercrime and prosecute perpetrators, and that efforts to obtain electronic evidence can benefit from international cooperation (Kello 2017, 199).

However, digital forensics remains locked in the logical layer of cyberspace. While law enforcement may be able to locate IP addresses and the wrongdoers behind it, investigation on their possible link to states remains considerably complex. To tackle this challenge, some specialists have argued in favour of establishing a multilateral mechanism of a technical nature dedicated to, and responsible for, the investigation of cyberattacks (Eilstrup-Sangiovanni 2018, 394-395; Clarke and Knake 2010, 252; Manshu 2022, 31; Chuanying 2022, 48).

If, as Nye argues, "[a]ttribution is a matter of degree" (Nye 2016-2017, 51), collective attribution by a mandated multilateral body, as opposed to unilateral attribution, would increase the credibility of cyber-investigations and their findings, as well as the legitimacy of imposing pre-established consequences for perpetrators.

A multilateral cybersecurity attribution/verification system could also support the overall regime in other ways. First, it would lock-in any successful

steps taken towards establishing clear norms and thresholds. Second, it could provide an efficient mechanism for sharing quality information, from states and its own internal investigations. Third, it could establish rules for how to address inconclusive cases, especially larger-scale attacks against critical infrastructure, including on when to refer them to international bodies mandated to assess threats to international peace and security. Fourth, it would allow for an institutional learning process (Nye 2016-2017, 51), regime self-improvement and accumulation of expertise. Fifth, such expertise could be channelled to assist countries' cyber-resilience efforts, as well as stimulate synergies with existing capacity-building programmes, saving resources and fomenting cross-learning processes.

Addressing the political challenges

The experience of the UN cybersecurity discussions demonstrates that there are at least two enduring circumstances that could lessen political resistances: existing systemic incentives and the role played by "middle-ground countries."

Systemic incentives

The informality of existing international cyber-norms makes them palatable for countries currently unwilling to tie their hands with international binding rules (Sukumar et al. 2024, 11). The fact that UN member states have recognized that international law applies to cyberspace – and therefore binds their cyber-activities – is not evidence to the contrary, since this application is still ambiguous (Chapter 2). As a result, there is a *de facto* informality regarding international obligations restricting state actions in cyberspace. This scenario seems to avoid strong resistance against further developing the existing framework of norms, pursued by the OEWG. In this vein, informality is not a weakness. As other experiences in the security area show, regimes may begin with voluntary measures and gain momentum towards stronger institutionalisation of norms of state behaviour (Nye 2018, 337).

Moreover, the increasing potential for disruption by cyber-weapons provides incentives for clearer rules of the game. The consensual norm prohibiting attacks against critical infrastructure is evidence that the international community is able to agree on such rules. Albeit informal and non-binding, existing norms can still exert a powerful influence over states (Nye 2016-2017, 61), as well as providing a blueprint for a future regime.

"Middle-ground countries"

In the UNGA cybersecurity discussions, the great majority of the states lie somewhere in the middle of the spectrum of interest and perspectives that separate the current global geopolitical rivals. Those states are identified sometimes as "middle-ground countries" (Buchan and Devanny 2024).

They play an active and influential role, bridging geopolitical divides and supporting capacity-building-based systemic stability. Many of them recall the two parallel (and potentially conflicting) processes established between 2019 and 2021 under the UNGA with a similar mandate to address cybersecurity.[6] There is a risk this duplication may reoccur after the mandate of the current OEWG expires in mid-2025. In 2022 and 2023, France and Russia tabled and managed to approve competing UNGA resolutions on the issue.[7] In 2023, warning against the divisiveness and "harmful duplication of efforts" this scenario causes, Brazil proposed a moratorium on such resolutions, in order to support the consensual work within the OEWG, in particular regarding the negotiations on the future mechanism that will succeed it (Brazil 2023). The Brazilian initiative gathered support, and, in 2024, a single resolution on cybersecurity was introduced and approved by the UNGA First Committee (United Nations General Assembly, A/RES/79/237, 2024).

Another example of influence comes from an informal group of fourteen Latin-American countries, according to which capacity-building is key to addressing overall cybersecurity challenges (see, for instance, Argentina 2021). These states have managed to influence the OEWG discussions, away from the assumption that cybersecurity is an end in itself, moving them closer to the view that it is an instrument for sustainable development. As seen in Chapter 2, capacity-building is now at the centre of the UN cybersecurity considerations.

Empirical evidence

The OEWG annual reports have reflected this Latin-American influence, including by giving capacity-building a central role in a future permanent UNGA cybersecurity interstate regular institutional dialogue (RID) mechanism (United Nations General Assembly, A/79/214, 2024, annex C, paras. 9-10). The negotiation of this mechanism is perhaps the main empirical evidence of UN member-states' current disposition in moving towards a global cybersecurity regime.

6 A GGE was established by UNGA Resolution 73/266, and an OEWG by UNGA Resolution 73/27.

7 UNGA Resolutions 77/37 and 78/16 (French initiatives), and 77/36 and 78/237 (Russian initiatives).

If approved, the RID mechanism would mark an important milestone in the global framework of addressing cyber-related issues and international peace and security. According to the latest OEWG report, "States recommend the establishment of the future permanent mechanism" and highlighted their willingness to "ensure a seamless transition from the OEWG to the future permanent mechanism" (United Nations General Assembly, A/79/214, 2024, para. 58).

This is significant. First, it could be a recognition that cybersecurity deserves – or imposes a need for – uninterrupted interstate dialogue, detached from specific, time-bound mandates, as with previous GGEs and OEWGs. Second, this would avoid the renegotiation of such new mandates. Third, it would avoid the possibility of having, once more, parallel fora in place with a similar mandate.

The current pace of the process is noteworthy. In 2023, states approved a first blueprint for this mechanism (United Nations General Assembly, A/79/214, 2024, paras. 55-57). In 2024, it was developed further, with general guiding principles, functions and scope, structure, modalities and a decision-making process (United Nations General Assembly, A/79/214, 2024, annex C, para. 10). Importantly, the mechanism is expected to have a focus on both (1) development of voluntary norms and of the understanding of how international law applies to cyberspace; and (2) capacity-building, "enabling States to secure ICTs and ensure their peaceful use" (ibid.).

Partial conclusion

Chapter 2 argued that a global cybersecurity regime is desirable. Its possible establishment and running would need, however, to be feasible. Experience shows that security regimes might need decades to emerge and mature. This Chapter has argued that, though technical and political challenges are significant, they are not insurmountable.

The recent experience at the UNGA is evidence that the international community is willing to tackle these challenges. In fact, the discussion of a global RID mechanism, under the UNGA, has picked up momentum, despite the current geopolitical circumstances. This is largely due to the systemic incentives (informality of the normative framework and urgency to address cyber-threats) and the work of the OEWG, in particular of the "middle-ground countries," which has managed to make notable progress by consensus.

It remains to be seen if the current momentum will drive the UNGA to approve a permanent RID mechanism to substitute the OEWG at the end of its mandate in mid-2025. The geopolitical scenario could deteriorate further, complicating an agreement. Furthermore, the existing technical challenges still need to be tackled, along with possible new hurdles derived from further technological developments.

Nonetheless, the progress made so far by the international community – establishing a framework of norms for responsible state behaviour and a blueprint for an RID mechanism – demonstrates the feasibility of and the appetite for a global cybersecurity regime aimed at promoting "an open, secure, stable, accessible, peaceful and interoperable ICT environment" (United Nations General Assembly, A/79/214, 2024, annex C, para. 4b).

Conclusion

This dissertation's goal was to address the question "to what extent could a global cybersecurity regime contribute to international peace and security?" This question is relevant because cyberspace has become another domain of interstate rivalry. Past cases of cyber-incidents have demonstrated the threat they represent, giving rise to defence and offense challenges and altering the international security environment. There is a lack of standards both for states to assess the alteration of the strategic landscape and for the "rules of the game" of interstate interaction in the cyber-dimension. This situation is prone to unprecedented volatile dynamics that may engender a security dilemma situation and uncontrolled escalation.

In this scenario, this work explored liberal institutionalist regime theory in order to seek ways to mitigate international instability stemming from cyberspace. Mindful of the role power politics play in the international system, its theorists stress that, while international regimes are no panacea, they still have value in avoiding violent international conflict.

In this vein, this work has argued that a global cybersecurity regime is desirable. A framework of incentives against malicious state behaviour could provide systemic stability if based on broadly agreed norms and on capacity-building efforts aimed at increasing systemic cyber-resilience. These two pillars would significantly alter cost-benefit perceptions and discourage malicious cyber-operations. In comparison, offensive domestic options could lead to motion security dilemma dynamics, especially dangerous given the opacity of cyber-capacities and societies' dependency on the constant and correct functioning of digital systems.

This dissertation has also argued that a global cybersecurity regime is feasible. However, two limitations should not be overlooked. First, Realists'

criticisms of regimes should be kept in mind. Power politics play a central role in influencing international security systems, let alone security regimes. As seen, power may influence their engines and overcome international legitimacy.

Second, a cybersecurity regime would face important technical and political challenges in its establishment and functioning, derived from the nature of cyberspace. Technical obstacles will demand significant engagement from the international community to arrive at common understandings on complex issues, such as on thresholds for cyber-operations deemed unacceptable, and on global mechanisms with legitimacy to investigate cyber-incidents, find culprits, and respond to violations. Political obstacles, such as states' resistance to reducing their autonomy, could be mitigated by enduring circumstances, such as the informality of the framework of norms of state behaviour and the increasing number of and harm done by cyber-attacks. Furthermore, the influence of "middle-ground countries" could help global rivals find agreements on sensitive issues and shift the focus of a possible regime towards cyber-resilience.

Finally, this work argued that the international community, through the OEWG/UNGA, has taken important steps towards a cybersecurity regime. In 2015, the framework of responsible state behaviour was established by consensus. In the past two years, these developments picked up momentum with the elaboration of a blueprint of a permanent RID mechanism, dedicated to cybersecurity, under the UNGA and open to all UN member-states. Taking Krasner's definition of regimes, 2025 may mark a critical milestone on the road towards a global cybersecurity one.

In sum, this dissertation asserts that a global cybersecurity regime is not only feasible but could provide a strong enough influence to discourage state-sponsored malicious cyber-operations and favour stability in the cyber-realm, thus contributing significantly to international peace and security.

Further research on this topic could entail related areas that fall beyond the scope of this work. This includes the impact on the international landscape of emerging technologies (especially artificial intelligence and quantum computing) and their fast development, as well as the role of non-state actors, in particular big techs. Further studies, departing from different IR perspectives, will likely contribute to how the current institutional developments, and the forces behind them, affect international phenomena.

Bibliography

Andres, Richard. "The emerging structure of strategic cyber offense, cyber defense, and cyber deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek Reveron, 89–104. Washington: Georgetown University Press, 2012.

Argentina. *Capacity building on behalf of a group of LAC countries*. United Nations Office for Disarmament Affairs, 2021. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-*(2021)/JS_Capacity_building_on_behalf_of_a_group_of_LAC_Countries*-_ENGLISH_VERSION.pdf.

Belk, Robert, and Matthew Noyes. *On the use of offensive cyber capabilities: a policy analysis on offensive US cyber policy.* Science, Technology, and Public Policy Program, Belfer Center, 2012.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power.* London: Routledge, 2011.

Brazil. *Statement by Brazil. "I Committee of the United Nations General Assembly", October 24, 2023*. https://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com23/statements/24Oct_Brazil.pdf.

Buchan, Russell, and Joe Devanny. *Cyber diplomacy in the middle ground*. Carnegie Endowment for International Peace. https://carnegieendowment.org/programs/technology-and-international-affairs/cyber-diplomacy-in-the-middle-ground.

Burgess, Matt. "Conti's attack against Costa Rica sparks a new ransomware era." *Wired,* June 12, 2022. https://www.wired.com/story/costa-rica-ransomware-conti/.

Canada. *International law applicable in cyberspace*. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.

Checkel, Jeffrey. "The constructive turn in international relations theory." *World Politics* 50 (1998): 324–348.

Chuanying, Lu. "A Chinese perspective on public cyber attribution." In *Managing US-China Tensions over Public Cyber Attribution,* edited by Ariel Levite et al., 43–63. Washington: Carnegie Endowment for International Peace, 2022.

Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers, 2010.

Comprehensive Nuclear-Test-Ban Treaty Organization. *Detecting nuclear tests*. https://www.ctbto.org/our-work/detecting-nuclear-tests.

Cyber Security Agency of Singapore. *ASEAN-Singapore Cybersecurity Centre of Excellence*. Last modified October 6, 2021. https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence.

Egloff, Florian. "Contested public attributions of cyber incidents and the role of academia." *Contemporary Security Policy* 41, no. 1 (2019): 55–81.

Eilstrup-Sangiovanni, Mette. "Why the world needs an international cyberwar convention." *Philosophy & Technology* 31, no. 3 (2018): 379–407.

European Union. *EU statement – UN Open-Ended Working Group on ICT in international law.* European External Action Service, May 24, 2023. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-international-law-1_en.

Fazal, Tanisha. "The power of principles: what norms are still good for." *Foreign Affairs,* June 2024. https://www.foreignaffairs.com/ukraine/power-principles-norms-tanisha-fazal.

Goodman, Will. "Cyber deterrence: tougher in theory than in practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102–135.

Hurel, Louise. "Interrogating the cybersecurity development agenda: a critical reflection." *The International Spectator* 57, no. 3 (2022): 66–84.

Hurwitz, Roger. "Keeping cool: steps for avoiding conflict and escalation in cyberspace." *Georgetown Journal of International Affairs* (2013–2014): 17–28.

International Atomic Energy Agency. *Safeguards implementation report for 2023*. June 7, 2024. https://www.iaea.org/sites/default/files/24/06/20240607_sir_2024_part_ab.pdf.

International Atomic Energy Agency. *Statute of the International Atomic Energy Agency.* October 23, 1956. https://www.iaea.org/sites/default/files/statute.pdf.

International Law Commission. *Draft articles on responsibility of states for internationally wrongful acts.* 2001. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

Jervis, Robert. "Cooperation under the security dilemma." *World Politics* 30, no. 2 (1978): 168–214.

Jervis, Robert. "Security regimes." *International Organization* 36, no. 2 (1982): 357–378.

Kello, Lucas. "The meaning of the cyber revolution." *International Security* 38, no. 2 (2013): 7–40.

Kello, Lucas. *Striking Back: The End of Peace in Cyberspace – and How to Restore It.* New Haven: Yale University Press, 2022.

Kello, Lucas. *The Virtual Weapon and International Order.* New Haven: Yale University Press, 2017.

Keohane, Robert. "The demand for international regimes." *International Organization* 36, no. 2 (1982): 325–355.

Keohane, Robert. *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton: Princeton University Press, 1984.

Keohane, Robert, and Lisa Martin. "The promise of institutionalist theory." *International Security* 20, no. 1 (1995): 39–51.

Kissinger, Henry, Eric Schmidt, and Daniel Huttenlocher. *The Age of AI: And Our Human Future.* New York: Little, Brown and Company, 2021.

Kissinger, Henry. *World Order.* New York: Penguin Press, 2014.

Krasner, Stephen. "Structural causes and regime consequences: regimes as intervening variables." *International Organization* 36, no. 2 (1982): 185–205.

Manshu, Xu. "Beyond public cyber attribution: reflections and response." In *Managing US-China Tensions over Public Cyber Attribution,* edited by Ariel Levite et al., 25–32. Washington, DC: Carnegie Endowment for International Peace, 2022.

Mazarr, Michael. *Understanding Deterrence.* RAND Corporation, 2018.

Mearsheimer, John. "The false promise of international institutions." *International Security* 19, no. 3 (1994–1995): 5–49.

North Atlantic Treaty Organization. *NATO 2022 Strategic Concept*. NATO, June 29, 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

Nye, Joseph. "Deterrence and dissuasion in cyberspace." *International Security* 41, no. 3 (2016–2017): 44–71.

Nye, Joseph. "Normative restraints on cyber conflict." *Cyber Security: A Peer-Reviewed Journal* 1, no. 4 (2018): 331–342.

Nye, Joseph. *The regime complex for managing global cyber activities.* Global Commission on Internet Governance. London: Chatham House, 2014.

Nye, Joseph. *The Future of Power.* New York: PublicAffairs, 2011.

Oosthoek, Kris, and Christian Doerr. "Cyber threat intelligence: a product without a process?" *International Journal of Intelligence and CounterIntelligence* 34, no. 2 (2021): 300–315.

Organization of American States. *CSIRTAmericas Network*. https://csirtamericas.org/en.

Patrick, Stewart. "NATO's deterrence problem: an analog strategy for a digital age." *Council on Foreign Relations,* August 2018. https://www.cfr.org/blog/natos-deterrence-problem-analog-strategy-digital-age.

Plummer, Robert, and Tom Gerken. "CrowdStrike and Microsoft: what we know about global IT outage." *BBC,* July 19, 2024. https://www.bbc.com/news/articles/cp4wnrxqlewo.

Rid, Thomas. *Cyber War Will Not Take Place.* Oxford: Oxford University Press, 2013.

Russian Federation. *Updated concept of the convention of the United Nations on ensuring international information security.* United Nations Office for Disarmament Affairs, 2021. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf.

Schmitt, Michael, and Liis Vihul. "The emergence of international legal norms for cyberconflict." In *Binary Bullets: The Ethics of Cyberwarfare,* edited by Fritz Allhoff et al., 34–55. Oxford: Oxford University Press, 2015.

Schöndorf, Roy. "Israel's perspective on key legal and practical issues concerning the application of international law to cyber operations." *International Law Studies* 97 (2021): 395–406.

Sheldon, John. "Deciphering cyberpower: strategic purpose in peace and war." *Strategic Studies Quarterly* 5, no. 2 (2011): 95–112.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press, 2014.

Standage, Tom, and Seth Stevenson. "Human insecurity." Produced by Slate. *Secret History of the Future,* October 3, 2018. Podcast, 0:30:11. https://slate.com/technology/2018/10/what-an-1834-hack-of-the-french-telegraph-system-can-teach-us-about-modern-day-network-security.html.

Stanič, Ana. "Bustani v. Organisation for the Prohibition of Chemical Weapons. Judgment No. 2232." *The American Journal of International Law* 98, no. 4 (2004): 810–814.

Strange, Susan. "Cave! Hic dragones: a critique of regime analysis." *International Organization* 36, no. 2 (1982): 479–496.

Sukumar, Arun, et al. "The pervasive informality of the international cybersecurity regime: geopolitics, non-state actors and diplomacy." *Contemporary Security Policy* 45, no. 1 (2024): 7–44.

Tikk, Eneken. "Future normative challenges." In *The Oxford Handbook of Cyber Security,* edited by Paul Cornish, 751–768. Oxford: Oxford University Press, 2021.

United Kingdom. *The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber-Intrusion Capabilities*. https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

United Nations General Assembly. *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Report of the Group of Governmental Experts*. A/76/135, July 14, 2021. https://undocs.org/a/76/135.

United Nations General Assembly. *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/RES/73/266, December 22, 2018. https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf.

United Nations General Assembly. *Definition of Aggression*. A/RES/3314(XXIX), December 14, 1974. https://undocs.org/A/RES/3314(XXIX).

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/70/237, December 30, 2015. https://undocs.org/A/RES/70/237.

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/73/27, December 11, 2018. https://undocs.org/A/RES/73/27.

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/75/240, December 31, 2020. https://undocs.org/A/RES/75/240.

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behaviour in the Use of Information and Communications Technologies*. A/RES/76/19, December 8, 2021. https://undocs.org/A/RES/76/19.

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/77/36, December 12, 2022. https://undocs.org/A/RES/77/36.

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/78/237, December 5, 2023. https://undocs.org/A/RES/78/237.

United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/10, July 30, 2010. https://undocs.org/a/65/201.

United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174, July 22, 2015. https://undocs.org/A/70/174.

United Nations General Assembly. *Official Compendium of Voluntary National Contributions on How International Law Applies to the Use of Information and Communications Technologies by States*. A/76/136, July 13, 2021. https://undocs.org/A/76/136.

United Nations General Assembly. *Open-ended working group on security of and in the use of information and communications technologies 2021–2025 established pursuant to General Assembly resolution 75/240*. A/RES/79/237, December 24, 2024. https://undocs.org/A/RES/79/237.

United Nations General Assembly. *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security*. A/RES/77/37, December 12, 2022. https://undocs.org/A/RES/77/37.

United Nations General Assembly. *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security*. A/RES/78/16, December 5, 2023. https://undocs.org/A/RES/78/16.

United Nations General Assembly. *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/79/214, July 10, 2024. https://undocs.org/A/79/214.

United Nations General Assembly. *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/78/265, annex C, August 1, 2023. https://undocs.org/A/78/265.

United Nations Institute for Disarmament Research. *Accelerating ICT Security Capacity Building: Take-Aways from the Global Roundtable on ICT Security Capacity Building*. June 2024. https://unidir.org/wp-content/uploads/2024/06/UNIDIR_Accelerating_ICT_Security-Capacity_Building_Take_Aways_from_the_Global_Roundtable_on_ICT_Security_Capacity_Building.pdf.

United Nations Office for Disarmament Affairs. *Programme of Action on Cybersecurity*. https://poc-ict.unoda.org.

United States Cyber Command. *Our History*. https://www.cybercom.mil/About/History/.

United States of America. *2023 Cyber Strategy of the Department of Defense*. September 12, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

World Economic Forum. *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.