The Journal of Military History and Defence Studies
Vol 4. Issue 1. (March 2023)
Maynooth Academic Publishing ISSN 2712-0171
http://ojs.maynoothuniversity.ie/ojs/index.php/jmhds

International Law and the Regulation of Cyberoperations Below the *Jus Ad Bellum* Threshold. An Irish Cybersecurity Perspective

Maeve O' Grady

Josep Borrell, Vice President of the European Commission, set out his fears that the EU was at risk of being "always principled but seldom relevant" (2021, p. 2). International law could be said to be similarly threatened, particularly in relation to cyberoperations, in respect of which its application has been strongly challenged. While states now broadly agree that international law applies in cyberspace, how it applies remains uncertain and contested. This paper analyses why the application of international law to cyberspace has been so fraught with difficulties and considers whether international law can provide the Irish State with a means of enhancing its cybersecurity and deterring state-led cyberoperations below the threshold of armed conflict.

The paper finds that the application of international law in cyberspace is problematic due to the manifestation of cyberoperations below the *jus ad bellum* threshold, and the challenging geopolitical environment that inhibits agreement on the principles of the international law of cyberoperations. International law is an object of dispute (Delerue, Douzet, & Gery, 2020, p. 15) and arguments on the application of international law in cyberspace represent states' strategic positions in the evolving geopolitical power struggle. The paper finds that, as cyberoperations are transnational, unilateral responses cannot be effective, and that small states have an interest in promoting international law and norms to create a more favourable international environment. The paper concludes that, as international law continues to exert a normative force on state behaviour, it has the potential to regulate sub-threshold cyberoperations as part of the comprehensive approach to cybersecurity.

The threat posed by state-led cyberattacks is one that challenges our national security, our personal safety and our economy. It is a global threat which, accordingly, cannot be addressed solely by unilateral action. International law is one facet of the comprehensive response, but its application in cyberspace is disputed and ambiguous. Cyberoperations below the threshold of armed conflict occur in a challenging and contested environment in which actors seek strategic advantage. It is an environment that is fluid and evolving and there is potential for multiple interpretations of acceptable state behaviour. One point of consensus in the debate relates to the absence of a coherent international legal response to cyberoperations. This paper will analyse international law to determine its utility in regulating state behaviour in cyberspace and improving Irish cybersecurity. It will consider the application of both international law and non-binding cyber norms to strategic cyber-competition. In order to do this, it will consider the

development of state-sponsored and state-enabled cyberoperations below the threshold of armed conflict, the *jus ad bellum* threshold, and it will review whether international law offers a remedy to the threats posed. This paper will not address criminal and sub-state actors in cyberspace. While these elements often have the capability to impact state security, a consideration would require an analysis of domestic law enforcement and transnational policing that is outside the scope of the paper. The paper, furthermore, does not seek to exhaustively consider how international law applies, but to analyse the applicable concepts as a framework for addressing the security challenges posed to the Irish State.

Literature Review

International Law of Cyberoperations

The regulation of cyberspace is complicated by uncertainty and disagreement surrounding the application of international law. Notwithstanding that the reach and specific application of international law is contested, a legal void does not exist in cyberspace. In 2021, the United Nations (UN) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (GGE) reaffirmed previous reports that "international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable … and peaceful… environment" (UN, 2021a, p. 8). The UN GGE had, however, failed to achieve consensus on its 2017 report due to disagreements on the application of international humanitarian law in cyberspace. In the wake of this failure, Russia proposed an alternative process that became the *Open Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security* (OEWG). The UN GGE and UN OEWG processes have since worked in parallel with similar mandates, albeit with the UN GGE largely Western sponsored, and the UN OEWG sponsored by Russia (Ponta, 2021, p. 2). These two parallel processes illustrate the geopolitical contestation and division that is influencing, and indeed impeding, the evolution and application of international law in cyberspace.

To promote a better understanding of how international law applies in cyberspace, the UN GGE requested participating nations to submit their national positions. The resulting *Official Compendium of Voluntary National Contributions on the subject of how international law applies to the use of information and communications technologies (ICTs) by States* (UN, 2021) (hereinafter called the *Voluntary National Contributions*) represents a step towards the clarification of the practical application of international law in cyberspace and the advancement of *opinio juris*. *Opinio juris* is the subjective belief that a state is bound to act in a particular way by international law. While this discussion on international law is positive and it has shaped the discourse on state behaviour in cyberspace, states have remained slow to act, and to explicitly declare that they are acting, according to specific principles of international law.

In the absence of clear state-led expressions on international law in cyberspace, non-state actors and institutions have attempted to address the lacuna. One example is the international group of experts that was sponsored by the North Atlantic Treaty Organisation's (NATO) Cooperative Cyber Defence Centre of Excellence (CCD COE) to develop a manual on the international law applicable to cyberoperations. The group produced two manuals on the subject as a guide to lawyers advising governments on cyberoperations. The *Tallinn Manuals* reflect the

consensus amongst the experts on the international law of cyberoperations as it stood at the time of drafting of the two manuals: June 2012 and June 2016 respectively. The manuals are, therefore, a statement of the existing law on those dates, or the *lex lata*, rather than an attempt to set out the direction of future law, or *lex feranda*. This could be considered a weakness in a sphere of operations where both the threat and the technology are evolving rapidly. The *Tallinn Manuals* can also be criticised for offering a NATO-centric or Western perspective of international law. As will be discussed later in the paper, international law is being challenged by contestation along geopolitical lines, which raises questions as to the universality of the law stated by the *Tallinn* experts.

Tsagourias believes that states have not been fully responsive to the *Tallinn Manuals* because states see themselves as the engines of international law and refuse to delegate this function to non-state actors (2019, p. 74). Efrony and Shany also question the degree to which the *Tallinn Manuals* are "universally regarded as an acceptable basis for articulating the norms of international law governing cyberoperations" (2018). Arguably, however, the *Tallinn Manuals* filled the gap created by the failure of states to expressly develop international law in cyberspace and they may have a normative effect on its development. Brazil, Germany, Japan, the Netherlands, and Norway expressly reference and rely on the *Tallinn Manuals* in their *Voluntary National Contributions* (UN, 2021). The *Tallinn Manuals* may not be binding, but they have proved persuasive.

The failure of states to actively lead the development of the international law of cyberoperations has not only led to an increase in informal international law making efforts such as the *Tallinn Manuals*, but it has also led to the rise of 'soft law' or non-binding norms. The 2015 UN GGE report included eleven non-binding norms that were intended to set standards for state behaviour (UN, 2015). Consensus on norms is easier to achieve in a contested international environment as they are explicitly non-binding. Norms do not directly lead to the development of *opinio juris* and the establishment of international law, but they can create expectations of behaviour that, with time, can crystallise into customary international law. Burchardt argues that norms create a yard-stick that can lead to an adjustment in behaviour to this standard, especially when there is no legal standard (2019, p. 305). Norms can thus compliment and shape the development of international law and their use to enhance cybersecurity will be addressed in this paper.

The potential for ambiguity, uncertainty, obfuscation, and opacity in relation to international law and norms in cyberspace is evident. It has allowed states and state proxies to compete vigorously for strategic advantage in cyberspace. Just as nature will fill a vacuum, the legal lacunas that exist will be exploited by actors who can take advantage of the absence of regulation.

The Fundamentals of Cyberoperations

Existing international law is faced with the difficulty that cyberoperations tend to challenge its fundamental structures. The leading writers on the characteristics of cyberoperations include Fishcerkeller, Harknett and Goldman (for example, Harknett & Goldman, 2016; Fischerkeller & Harknett, 2017; Fischerkeller & Harknett, 2018). In 2018, in response to their writings on the fundamental characteristics of cyber-contest, United States (US) cyber policy shifted significantly

to address the emerging reality of persistent cyberattacks below the *jus ad bellum* threshold (US Cyber Command, 2018, p. 2). Consideration of these elements has remained very much US centred. Liebetrau (2022) attempts to redress that balance by assessing how three European Union (EU) states perceive and respond to cyber conflict short of war. There is limited further consideration of strategic cyber-contest below the threshold of armed conflict from a European perspective.

Small State Cybersecurity

Keohane's *Lilliputians' Dilemma* gives food for thought on both the definition of small states and on small state security models (1969). Keohane was, however, writing at a time when territorial integrity, rather than cybersecurity, was the primary challenge for small states and traditional small state security literature tends, naturally, to focus on military security rather than on 'soft' security threats. Burton and Tan have, however, addressed this issue, with Burton writing on cybersecurity in New Zealand, while Tan considers Singapore's situation. Burton applies models of small state security to cybersecurity and concludes that strategic rivalries are hampering the use of international institutions as models of small state security (Burton, 2013, p. 222). As this is a quickly moving field of study, his research is now somewhat in need of updating, however, it provides an original approach to considering small state cybersecurity. Tan (2018; 2020) writes about cybersecurity from a Singaporean perspective, and while Singapore operates in a different geopolitical context to Ireland, it can offer insights into the challenges of a small, developed and interconnected state in tackling cybersecurity.

Research Lacunae

The literature overview illustrates the problematic application of international law to cyberspace and that little consideration has been given to assessing whether international law can enhance small state cybersecurity. This paper attempts to add to the cybersecurity debate by introducing considerations of the role of international law in contributing to cyber deterrence and to small state security from the Irish perspective. The paper will set out the nature of the cyberthreat facing Ireland and will analyse the contribution and relevance of international law to concepts of small state cybersecurity. This paper will, therefore, advance the discussion by framing an analysis of the international law of cyberoperations against an Irish cybersecurity paradigm.

Research Questions

The research objective is to analyse international law to determine its utility in regulating state-led cyberoperations below the *jus ad bellum* threshold and its relevance to Irish cybersecurity. In order to address this question, a number of subsidiary questions will be considered. First, why do cyberoperations present such a challenge for international law? Secondly, is international law a valid tool for regulating international cyber interactions in the face of challenges to multilateralism and rising geopolitical competition? Thirdly, if international law struggles to regulate cyberoperations, what gaps have emerged and should other means of regulating state behaviour, for example, non-binding norms or a cyber treaty, be considered? Finally, can international law contribute to models of small state security and to cyber deterrence?

Methodology and Sources

The paper utilises a qualitative analysis of primary legal rules and leading academic commentary on international law. Secondary sources on international law and on cyberoperations have also been examined to contextualise and explore these issues more fully. This method is supplemented by a comparative analysis of states' expressed positions on the international law of cyberoperations to identify common ground or areas of divergence. The fundamental nature of cyberoperations is explored to consider how international law applies to cyberoperations, and how its application is shaped by the geopolitical environment in which it operates.

PART ONE: The International Law of Cyberoperations: A Square Peg in a Round Hole?

The discussion above has established that international law applies to cyberspace in principle, but that its practical application remains somewhat elusive. This section explores the extent to which international law provides a capable means of regulating state behaviour in cyberspace. The objective of Part One is to identify how cyberoperations manifest, to differentiate cyberoperations from conventional kinetic threats, and, thereby, to consider the application of international law to cyberoperations.

This Part is divided into two sections. Section one addresses the nature of cyberoperations and their unique characteristics including first, strategic competition below the threshold of armed conflict, and secondly, constant, non-discretionary contact with adversaries. These characteristics challenge the applicability of international law, which evolved to govern the use of kinetic force in the so-called "conventional strategic environment" (Fishcerkeller, 2021). Section two considers the challenge to the legitimacy and efficacy of international law and the rules-based international order. Part One thus contextualises the current reality of both cyberoperations and international law and considers how these elements interact.

The Nature of Cyberoperations: Sub-Threshold and Persistent

Two key characteristics of the cyber-environment will be addressed here. The first is strategic contest below the threshold of armed conflict. The second is persistent and non-discretionary contact with adversaries. It is argued that these fundamental characteristics drive the scale and scope of cyberoperations, the grey zone cyberattacks, that states are subject to on a daily basis. Thus, the use of cyberoperations as a strategic alternative to war, and the security implications thereof, will be considered.

Strategic Sub-Threshold Contest

Lawful recourse to armed force is determined by the *jus ad bellum*. Article 2(4) of the UN Charter explicitly prohibits the "… *threat or use of force* against the territorial integrity or political independence of any State…(emphasis added)" (United Nations, 1945). The concept of sovereignty is, therefore, central. The prohibition can be derogated from in two principal scenarios. The first is where the Security Council authorises the use of force to maintain or restore international peace and security under Chapter VII of the UN Charter. The second exemption is under Article 51 which provides for the "…inherent right of individual or collective self-defence if

an *armed attack* occurs against a Member of the United Nations...(emphasis added)" (United Nations, 1945). There are other limited exceptions where force may be used, however, the concepts of use of force, armed attack and sovereignty are central. These concepts are difficult to define in the context of cyberoperations and the thresholds for meeting these tests in cyberspace are uncertain. It is not impossible that a cyberattack could reach the *jus ad bellum* threshold, however, a focus on a single dramatic event that does so, the "*black swan*" cyberattack, ignores the reality of strategic cyber-contest which is incentivised to manifest below the threshold of armed conflict.

In the early 1990s, Arquilla led the scholarly debate on the coming cyberwar (for example; Arquilla & Ronfeldt, 1993). Others, notably Rid, argued, however, that no cyberattack meets the Clauswitzean criteria of violent, instrumental, and political. Rid argues that cyberattacks can never be war and are, instead, more sophisticated versions of subversion, espionage, and sabotage (2013, p. xiv). According to Rid's perspective, cyberattacks have always been, and are likely to remain, below the *jus ad bellum* threshold. Harknett (2018) argues that states act intentionally below the threshold of armed conflict as they can achieve strategic effect "without territorial aggression or the threat thereof". Harknett and Smeets go further and argue that cyberoperations should be viewed "not as enablers of war, although they can be, but more critically as the strategic alternative to it" (2020, p. 2). Cyberoperations are designed to exploit vulnerabilities and weaknesses in our systems, both technological and societal, and are utilised, not to compel an adversary to submit by force, but to undermine, to sabotage, to sow discontent and to strategically weaken without the use of force. Although cyber is an inherent enabler of military capability across the operational domains, state-use of cyberoperations manifests in sub-threshold activities. This is not to ignore the potential uses of cyberoperations in war, however, the daily reality is that of sub-threshold cyberoperations.

Operating below the *jus ad bellum* threshold negates the military dominance of larger powers and restricts the application of the full range of international law. As illustrated in the introduction, states have come to agree that international law applies in cyberspace but not the specifics of its application. Cyberattacks can be directed into that unregulated grey zone and can achieve strategic gain by doing so with little recourse available. Fishcerkeller points out that it is unsurprising that international law that was "conditioned by the nuclear and conventional strategic environments struggles to be relevant in the cyber strategic environment" (2021). Thus, the incentivisation of cyberoperations below the threshold of armed conflict is clear and Ireland is likely to continue to face these types of cyberoperations.

Constant and Non-Discretionary Engagement

Constant engagement with adversaries is another notable feature of cyberoperations and is caused by the nature of cyberspace, which is both interconnected and has inherent vulnerabilities that can be exploited on a mass scale. Harland and Hemsley describe it as "non-discretionary contest" (2019, p. 148). Fischerkeller and Harknett argue that cyberoperations are persistent because the cyber environment has vulnerabilities that allow actors to have strategic effects, but they can carry out these effects continually, without destabilising the cyber-environment as a whole. They state that;

> Through significant experimentation, states have discovered that the combination of system resiliency and vulnerability enables the realization of strategic gains through competition via cyber operations and campaigns short of armed conflict, thus presenting a *strategic incentive* for continued activity and further experimentation (2020).

The exploitation of vulnerabilities and the interconnected nature of the environment allow access to instruments of national power, incentivising constant probing. There is, furthermore, little downside to persistent probing if strategic advantage can be achieved through trial and error without causing an armed conflict and without destabilising the whole environment.

Constant engagement is further incentivised by the fact that private companies provide much of the global cyber-architecture and access is ubiquitous. Harknett and Goldman describe it as an "offense-persistent strategic environment" (2016, p. 86) in which there is constant contact with the enemy and an environment that is highly integrated into global society, unlike in traditional military environments (2016, p. 83). The UK's *Future Operating Environment 2035* outlines that "[t]he number of entry points and its decentralised and dispersed nature will mean that cyberspace is likely to remain porous and vulnerable to disruption" (Ministry of Defence UK, 2015, p. 20). It concludes that, even if states are willing and able to exercise jurisdiction over ICT infrastructure, they "lack full control because of the seamless boundaries across which information moves globally" (Ministry of Defence UK, 2015). Entry is both easy and cheap, allowing "non-state actors and small states [to] play significant roles at low levels of cost" (Nye, 2011, p. 20). Fischerkeller and Harknett argue that, while only a handful of states can "…operate with consequence in the land, air, maritime and space operational domains", in cyberspace that number is exponentially greater (2017, p. 382). They also argue that "operational persistence/engagement becomes a strategic imperative for states seeking to secure and advance their interests in …cyberspace" (2018, p. 3). Constant engagement prevents withdrawal or distancing from the adversary and allows weaker states to exert influence without costly conventional means and without the necessity to control territory. The use of cyberattacks by states including Iran, North Korea, and Russia illustrates their perceived utility as a means of achieving asymmetric advantage against stronger opponents.

The Manifestation – Grey Zone Cyberoperations

The structural incentivisation for persistent engagement below the threshold of war manifests in grey zone activities. In the context of this paper, the term 'grey zone' is used to describe state operations for strategic advantage below the threshold of armed conflict. Fischerkeller and Harknett refer to it as the "strategic competitive space between war and peace" (2018, p. 22). Strategic competition, involving sabotage, subversion, and the undermining of political systems, is conducted persistently through and via cyberspace. Further, it is not simply that cyberoperations tend to occur in the grey zone but as illustrated above, cyberoperations are incentivised to occur in the grey zone. Babbage (2019) uses the term political warfare to describe "operations to influence, persuade and coerce nation states, organisations and individuals to operate in accord with one's strategic interests without employing kinetic force". This description is highly correlative to grey zone activities as described here. Grey zone attacks can damage civilian infrastructure, undermine political systems, spread discontent, and damage the economy and reputation of a state, without triggering an armed response. These activities, outside the

traditional concepts of conventional force, are destabilising and damaging, but also limit the capability of the victim state to respond effectively and lawfully.

The threat from sub-threshold, or grey zone, cyberattacks is evident. The report into the 2016 US presidential election found that a group linked to the Russian Government "used social media accounts and interest groups to sow discord in the US political system..." (Mueller, 2019, p. 4). The report on the 2020 US presidential elections concludes that President Putin authorised influence campaigns in support of President Trump, "undermining public confidence in the electoral process, and exacerbating socio-political division in the US". It also concluded that Iran had attempted to create confusion and undermine the legitimacy of the elections (National Intelligence Council, 2021, p. 4). The EU has also been the target of such cyberoperations. In September 2021, the EU formally attributed Russia with the *Ghostwriter* cyberattack, which targeted the political systems of several member states. The EU stated that the attack sought "to threaten our integrity and security, democratic values and … the core functioning of our democracies" (Borrell, 2021). The European Commission warned in its *Democracy Action Plan* that Russia and China "have engaged in targeted influence operations and disinformation campaigns around COVID-19…seeking to undermine democratic debate, exacerbate social polarisation and improve their own image" (2020). Other examples that illustrate the imperative towards strategic sub-threshold cyberoperations include the *Stuxnet* attack on Iran in 2010 that was linked to the USA and Israel (CFR, 2010), the *WannaCry* attack in 2017 that was linked to North Korea, and the *NotPetya* attack in 2018 that was linked to Russia (EU Council, 2020). These attacks reflect the reality of today's cyber-campaigns and the manifestation of the characteristics of cyber-contest; constant, non-discretionary contact and sub-threshold strategic competition.

The Utility of International Law

This section will consider how international law is being challenged, not just by the new reality of cyberoperations, but by the contestation of the very fundamentals of the rules-based international order. Debate persists about whether international law is a relevant and effective means of regulating state behaviour and the current complex security environment appears to have created a crisis of legitimacy surrounding international law. Bruneé (2018) believes that the challenges to international law today are more corrosive and dangerous than seen for some time. The apparent return to realist power politics challenges international law, and Koh (2019) argues that we are witnessing a battle between the Kantian vision of a law-governed international society and a more cynical Orwellian vision of realist great power competition. According to Wouters, the rise of populism in the West has seen Western democracies become increasingly reluctant to promote multilateralism and the rule of law (2019, p. 244). Wouters was writing during the Trump presidency, when populism appeared to be inexorably rising. Without the benefit of a longer view of history, it is not clear whether Trumpism and Brexit represented the zenith of populism, however, for now, it continues to influence political and social discourse. Wouters also argues that international law is assumed to be universally shared, but that it, in fact, reflects Western world views and, as power shifts towards non-Western states, certain basic norms are being questioned (2019, p. 255). International law is founded on universalism and the undermining of multilateralism diminishes that universality.

The EU's *Strategic Compass* recognises that the rules-based international order "has come under strong questioning, through the shattering of universal values and a lopsided use of

global challenges, by those promoting a strict sovereigntist approach that constitutes in reality a return to power politics" (Council of the EU, 2022, p. 7). This sovereigntist approach is reflected in developments in cyberspace. The UN GGE failed to reach a consensus report in 2017 due to an impasse on how international law applies in cyberspace. In the wake of that failure Brazil, Russia, India, China, and South Africa (the BRICS states) concluded a declaration recognising that international law applies in cyberspace, albeit, with an emphasis on state sovereignty and non-interference. In the declaration, they stated:

> We emphasise the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly the state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms. (BRICS, 2017)

Similarly, the *Voluntary National Contributions* on international law in cyberspace by both Russia and China, while recognising the applicability of international law to cyberspace, stress the principles of non-intervention and state immunity (UN, 2021). Thus, while international law is respected in the statements, its application is restricted to a narrow sphere.

It appears, therefore, that international law is being challenged by an undermining of multilateralism, a sovereigntist approach by some states, and by the shifting geopolitical balance of power. International law lends itself to contestation as it has an inherently political and strategic dimension that is not present in domestic law. Its potential for interpretation and ambiguity can lead to its instrumentalisation as a means of protecting or projecting state power. China's actions in seeking to misapply and misinterpret international law in the South China Seas for its own benefit are illustrative. International law is, therefore, a "strategic object, used and sometimes manipulated by a state based on its perception of a national interest" (Delerue, Douzet, & Gery, 2020, p. 14, citing Fernandes, 2011). Thus, while international law has a role in moderating state behaviour, it cannot be thought of as occurring in a vacuum, devoid of real-world implications.

The challenges to international law are not new and, in 1988, Kertzer warned against "the naïve notion that politics is simply the outcome of different interest groups competing for material resources" (1988, p. 174). Arguably, this remains valid. Maçák, citing a study by Crawford on the effectiveness of international legal obligations, argues that it is more likely that states will act in accordance with standards of behaviour when it is required by law than when it is not (2017, p. 887). The desire to be seen as legitimate, and to exercise influence through that legitimacy, encourages state-adherence to international law when they might otherwise act differently. While Realists may argue that great powers will not adhere to international law when it is not in their interests, such a perspective does not adequately explain the general compliance with international law, nor does it explain why states limit their freedom of action by entering and adhering to voluntary treaties and conventions. Constructivists believe in the power of principled ideas and see international law as the scaffolding on which the rules of state behaviour are built (Hathaway, 2005, p. 481). Hart, in his defining work *The Concept of Law*, suggests, however, that trying to understand compliance with the law, either through the simplistic lens of an order backed by threats, or the complex concept of morality, risks obscuring the features

which distinguish law from other means of social control (2012, p. 271). Hart reframes the issue in terms of whether international law gives rise to meaningful obligations.

Adherence to the UN Charter and to multilateral treaties, public declarations by states on international law, and the existence of *opinio juris*, all indicate that states think of, speak of and act as if international law is binding and it, thus, provides a normative force in regulating state behaviour. While it is often transgressed, even in its transgression, states continue to use the language of international law. The International Court of Justice (ICJ) points out that;

> If a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then … the significance of that attitude is to confirm rather than to weaken the rule (*Case Concerning Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), [1986] ICJ Rep 14, 186).

Even though violations of international law occur, Henkin argues that these "…are not common enough to destroy the sense of law, of obligation to comply, of the right to ask for compliance and to react to violation" (1979, p. 89). The powerful may violate international law when absolutely in their interests, but a state's perception of when that point arises will necessarily consider the costs of breaching the law. The interests of power and law may not always coalesce, but power is shaped and harnessed through lawful action and, indeed, power is often exercised through legal regulation. International law does not guarantee conformity to its requirements, but it does increase the stakes for a state that is considering breaching international law. Keohane argues in relation to international organisations, that state behaviour determines the nature of international systems as well as *vice versa* (1969, p. 295). It can also be argued that international law, while it is shaped by state behaviour, it also shapes state behaviour, and this is a positive starting point in the discussion on increasing security in cyberspace.

Cyberspace is often seen as a global commons, an area falling outside the jurisdiction of any one state and one to which all states have access. This may not be a fully accurate description of cyberspace as states have sovereign authority over cyber infrastructure, persons, and activities within their territories (UN, 2013; UN, 2015), but it is inherently a space in which the actions of one state can impact on another. There must, therefore, be increased coherence and collective agreement as to acceptable state behaviour. While international law has deficiencies, both generally and in respect of the regulation of cyberoperations, it offers at least the possibility of a framework to address them. Borrell states that "the threats we face around the world are intensifying and the capacity of individual [EU] Member States to cope is insufficient and declining" (2022, p. 4). The EU has acknowledged that the defence of Europe requires a new comprehensive concept of security, and international law is one part of that comprehensive approach. That is not to ignore the reality of the challenges to international law and the contestation of its rules and norms. These challenges should not undermine the general legitimacy of international law, although it is acknowledged that significant work is required to achieve international agreement on the practical application of international law to cyberoperations.

Conclusion

It is argued that the key features of cyberoperations include constant engagement and sub-threshold competition. These are incentivised by the nature of the cyberspace environment, with its inherent vulnerabilities in a resilient whole, low cost of entry, a multiplicity of actors, access to levers of national power, the ability to achieve strategic gain without the use of force, and a structure that is not controlled by the state or its organs. These factors manifest in sub-threshold cyberoperations that have the potential to destabilise, undermine and sabotage. The title of this Part asked whether the international law of cyberoperations is a square peg in a round hole? It establishes that international law is challenged by the fundamental characteristics of cyberoperations that have facilitated widespread strategic sub-threshold competition. International law is further challenged by the geostrategic environment and a seeming return to Realist power politics. It is argued, however, that international law remains a normative force in regulating state behaviour, and that the transnational threat posed by cyberoperations creates an imperative for multilateral cooperation to regulate cyberspace. While it is imperfect and not fully aligned to the cyber-environment, international law potentially offers one part of the comprehensive response to sub-threshold cyberoperations.

PART TWO: Applying International Law to Sub-Threshold Cyberoperations

Part One identified how cyberoperations challenge international law specifically, while acknowledging the contested nature of international law more generally. Part Two will analyse how the dual challenges identified affect specific rules of international law and will highlight limitations and areas for potential agreement. This Part is divided into three sections. It will first, broadly consider the lack of state practise in cyberspace, before, secondly, addressing the application of specific principles of international law. This will not be an exhaustive exploration of international legal principles, but rather a consideration of those principles that are applicable to sub-threshold cyberoperations. Furthermore, the intent is not to frame the exact parameters of each principle, but to set out their applicability and to highlight areas of controversy or disagreement. In this regard, the *Voluntary National Contributions* to the UN will be used to ground state positions. Thirdly, Part Two will consider the use of cyber norms and the utility of a cyber treaty to enhance security in cyberspace.

State Practice in Cyberspace

While there are treaties that govern state interactions, for example on the high seas and in outer space, there is no treaty that codifies state relations in cyberspace. As a result, the applicable law must be determined from existing international legal obligations, most of which developed long before the technology of cyberoperations had emerged. Accordingly, the contours of international law do not fit easily with the use of cyberoperations.

Customary international law requires the two pillars of general and consistent state practice and *opinio juris* (Wilt, 2019, p. 784). The full breadth of international legal rules governing cyberspace has, however, not been demarcated through state practice and *opinio juris*. Some commentators argue that states are taking a “wait and see” approach to the manner in which cyberoperations ought to be regulated as they assess their strategic utility (Maçãk, 2017,

p.881; Efrony & Shany, 2018, p. 584). Väljataga argued as recently as 2018 that "*opinio juris* of any kind… is either contradictory or classified to the point of being undetectable" (2018, p. 4). The UN is taking steps to address this issue through the *Voluntary National Contributions* (UN, 2021). These are an important starting point in determining national positions, however, the specific application of international law, even in light of these positions, remains problematic.

International Law Principles Below the *Jus Ad Bellum* Threshold in Cyberspace

Below the *jus ad bellum* threshold, concepts such as the "use of force" and "armed attack" have less utility, therefore, principles including sovereignty, non-intervention, due diligence, and attribution take on added importance. The parameters of these key principles become the defining legal boundaries, however, as will be illustrated, those parameters remain uncertain or contested.

Sovereignty

Sovereignty is a core principle of international law, and it encompasses the right of a state to exercise within its territory "to the exclusion of any other state, the functions of a state" (*Island of Palmas* (*Netherlands v. US*) 1928 2 RIAA 829, p. 838). Sovereignty, therefore, has a territorial aspect and so it is a challenging concept in cyberspace, which is not delineated by state boundaries. The UN GGE Reports of 2013 and 2015 both recognised, however, that state sovereignty applies to activities in cyberspace and to state jurisdiction over ICT infrastructure within their territory (UN, 2013; UN, 2015).

There are divergent opinions on the principle itself. The prevailing view is that sovereignty is a substantive primary rule of international law, the breach of which is an internationally wrongful act (Väljataga, 2018). The UK's position, however, is that sovereignty is a principle from which other principles of international law derive (UN, 2021, p. 117). Under this approach, which is also espoused by elements of the US Government (Corn & Taylor, 2017), a cyberoperation would have to violate another substantive principle of international law to constitute a violation of sovereignty. Schmitt and Vihul argue that this approach is intended to give states that are active in cyberspace the freedom to conduct attacks up to the threshold of, for example, the use of force or non-intervention (2017, p. 214). The ICJ has found, however, that activities that do not reach the threshold of an unlawful intervention or a use of force can still amount to a breach of sovereignty (for example *Certain Activities carried out by Nicaragua in the Border Area* (*Costa Rica v. Nicaragua*) [2015] ICJ Rep 665, para 229), so the UK's approach is a minority one. Nonetheless, the UK was willing to call out the Russian cyberattacks against the Ukrainian financial sector in February 2022 as showing "continued disregard for Ukranian sovereignty" (UK National Cyber Security Centre, 2022).

Even if it is accepted that sovereignty is a primary rule of international law, its practical application is unsettled. *Tallinn 2.0* takes the approach that a violation of sovereignty is determined on two grounds. The first is where there is physical damage, injury, or a loss of functionality, but the threshold for such damage, injury or loss of functionality was not agreed by the *Tallinn* experts (2017, p. 21). The "threshold of damage" approach is supported by some state-contributions to the UN and Norway, for example, outlines that a cyberoperation "may, depending on its *nature, the scale of the intrusion and its consequences*, constitute a violation of

sovereignty (emphasis added)" (UN, 2021, p. 67). The second ground for a violation of sovereignty is where there has been an interference with, or usurpation of, inherently governmental functions (*Tallin Manual*, 2017, p. 21). This is based on the *ratio* in the *Island of Palmas*. This view was endorsed by Germany (UN, 2021, p. 33) and the Netherlands, amongst others, in their *Voluntary National Contributions*, although the Netherlands highlighted that the precise boundaries of what constitutes a breach of sovereignty has not yet crystallised (UN, 2021, p. 56). The *Tallinn 2.0* experts suggested that an interference with "inherently governmental functions" could encompass cyberoperations that interfere with data or services necessary to deliver social services, conduct elections, or perform necessary defence activities (2017, p. 22).

Chircop proposes that all cyberoperations that interfere with a target state's cyber infrastructure violate sovereignty as long as the effects are more than "*de minimus*" (2019, p. 14). France has not made a submission to the UN but, in a previous paper, appears to take a similar position and states that "[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means…[that are attributable to a State]… constitutes a breach of sovereignty" (Ministère des Armées, 2019, p. 7). As outlined previously, Russia and China also hold sovereignty as a cornerstone of interactions in cyberspace and are likely to invoke a violation of sovereignty against activities of even a minimal kind.

The principle of sovereignty illustrates the problematic application of international law in cyberspace. Even the nature of the principle is contested and state views on the threshold to determine a violation of sovereignty are conflicting. In the absence of agreement, determining whether there has been a violation of sovereignty in cyberspace becomes a subjective decision, rather than being guided by an agreed understanding of the rule. The divergences of opinion also highlight the difficulty in getting agreement on principles of international law as a precursor to establishing *opinio juris*.

The Prohibition of Intervention

Non-intervention protects states from outside unlawful intervention and states may not interfere coercively, including by cyber means, in the internal or external affairs of another state (UN, 2021, p. 25, p. 34). The ICJ in its judgment in the *Nicaragua Case*, sets out that the purpose of the prohibition of intervention is to ensure that all states remain free from external "coercive intervention" in matters affecting a state's powers that are at the heart of a state's sovereignty. These functions include a state's choice of political, economic, social, and cultural system, as well as the formulation of foreign policy (*Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*) [1986] ICJ Rep 14).

The principle can govern both forcible and non-forcible coercion and it is, therefore, important in the context of sub-threshold cyberoperations. Estonia sets out that a prohibited intervention is one that "coerces a state to take a course of action it would not voluntarily seek" (UN, 2021, p. 25). Persuasion, criticism, propaganda, retribution, or maliciousness will not amount to coercion (*Tallin Manual*, 2017, p. 319). A more expansive approach is preferred by some commentators, however. Corn, for example, argues that the true objective of the rule is to prevent a state from being deprived of the free exercise of its will over sovereign matters and the prohibition can, therefore, be utilised to prevent deception, disruption, and information conflict (2020, p. 4). In its *Voluntary National Contribution*, Germany states that the spreading of

disinformation that may incite political upheaval or the disabling of election infrastructure would be equivalent to coercion in non-cyber contexts. Germany acknowledges, however, that it is difficult to formulate exact criteria due to the complexity of such cyberattacks (UN, 2021, p. 35). The release of emails from the Democratic National Committee (DNC) prior to the 2016 US presidential election is a useful illustration of the principle. A report by the Office of the Director of National Intelligence (ODNI) found that President Putin had ordered, through the General Staff Main Intelligence (GRU), a large scale cyberoperation "to undermine public faith in the US democratic process" and to "help President-elect Trump's election chances when possible by discrediting Secretary Clinton" (2017, p. ii). The Department of Defense issued a memorandum in January 2017 that affirmed that coercion is a prerequisite for a prohibited intervention and concluded that grey zone cyberoperations are "largely unregulated by international law at this time" (Department of Defense, 2017, cited by Banks, 2017, p. 1501). The DNC hack was not deemed a prohibited intervention and, therefore, the possibility of countermeasures was precluded. The lack of clarity as to what amounts to a prohibited intervention essentially allowed Russia to act with impunity.

As with sovereignty, the threshold of coercive behaviour has not been delineated. As more states set out their positions on non-intervention, the standard may evolve to govern circumstances such as the DNC hack. The US in its *Voluntary National Contribution* states that a cyberoperation "that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule" (UN, 2021, p. 140). Such statements may set the scene for future responses to election meddling. Therefore, while in its current state the prohibition of intervention is a narrow rule of international law, it has the potential to become an important element in responding to grey zone cyberattacks.

State Responsibility and Attribution

The customary international principle of state responsibility means that a state is responsible for acts that are internationally wrong and that can be attributed to that state. The principle has been codified in the *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* (hereinafter called the *Articles on State Responsibility*).

Attribution.

Attribution of a wrong is a necessary precondition to determining state responsibility. Attribution is, however, difficult from a technical, political, and legal perspective. Banks argues that international law on state responsibility and attribution fails to provide prescriptive norms that will help deter malicious cyberoperations (2017, p. 1495). The uncertainties of attribution further incentivise grey zone cyberattacks as attacks can be met with denials, both plausible and not.

While attribution can be difficult, states have been willing to attribute malicious cyberattacks. Recent examples include the US, the EU, NATO, and other world powers attributing the 2021 Microsoft Exchange hack to the Chinese government (Alperovitch & Ward, 2021). In July 2021, the FBI and the US Cybersecurity and Infrastructure Security Agency (CISA) attributed a spearfishing attack which took place between 2011 and 2013 to China (Centre for Strategic & International Studies, 2021). In October 2019, more than twenty states attributed a cyberattack on Georgian Government websites to Russia (Centre for Strategic & International Studies, 2021).

A clear articulation of standards of attribution and unambiguously outlined parameters of unacceptable behaviour can promote greater predictability and stability in cyberspace.

Non-State Actors.

To circumvent attribution, states can exploit the anonymity and difficulty of tracing cyberattacks by utilising non-state actors to achieve their strategic goals. Non-state actors are not constrained by international law, but their acts can be attributable to a state in certain circumstances. Articles 4, 5 and 6 of the *Articles on State Responsibility* specify that the acts of organs of the state, or of persons empowered by domestic legislation to exercise governmental authority, are attributable to a state (International Law Commission, 2001). Of more importance in targeting states using non-state actors as proxies, Article 8 provides that a state will be responsible if persons or groups act "on the *instructions* of, or under the *direction* or *control* of, that State in carrying out the conduct (emphasis added)" (International Law Commission, 2001). It is sufficient to establish any one of the three elements set out in Article 8, although none of them are defined in the text (International Law Commission, 2001, commentary to article 8, para 7).

There is caselaw and extensive academic commentary on the meaning of these three elements, however, for the current purposes, Mačák's conclusion is sufficient that the key element to all three parts (instructions, direction, control) is that there is "a subordinate relationship between the state and the private actor" (2016, p. 427). *Tallinn 2.0* sets out that general support or encouragement of cyberoperations, or assisting with particular functions or activities, is not sufficient to meet the test (2017, p. 97). Mačák takes a similar view and argues that "the fact of a goal shared by the state and the private actor is insufficient without further evidence of establishing the subordination between the two" (2016, p. 415). This implies that activities, including training, support, and a shared goal, would not suffice. States cannot evade responsibility by using non-state actors to achieve their goals, however, the bar is set very high for attributing a state with responsibility for non-state actors. This may allow non-state actors that are highly integrated in the state machinery to evade attribution on behalf of their state.

The Due Diligence Principle

The due diligence principle becomes useful if the acts of non-state actors cannot be attributed to a state. This principle confers a duty on a state to exercise due diligence by not allowing its territory to be used to cause serious adverse consequences to, or affect the rights of, other states (*United States v. Arjona* (1887) 120 US 479; UN, 2021, p. 26). There is a view, however, held by a minority of states including the US and UK, that there is insufficient *opinio juris* to support a claim that due diligence constitutes a binding obligation under international law and it is instead to be considered a norm (UN, 2021, p. 141).

Due diligence extends to cyberoperations conducted by non-state actors that are "contrary to the rights" of the affected state and have "serious adverse consequences" (*Tallin Manual,* 2017, p. 34). The term "contrary to the rights" of the affected state is drawn from the judgment in the *Corfu Channel Case* and means that the violation must be one that is contrary to international law and not merely a breach of domestic law (*Corfu Channel* (*UK v. Albania*), 1949 ICJ 4, p. 22). The *Tallinn 2.0* experts could not agree what constituted the exact definition of "serious adverse consequences" but gave examples of cyberoperations that result in severe

disruption to online banking, media, governmental functions, or business, as potentially coming within the meaning, illustrating that physical harm is not required (2017, p. 38). The cyberattack must, therefore, violate an international law principle and must have serious adverse consequences, although the precise meaning remains undefined.

The *Corfu Channel Case* makes it clear that the territorial state must have knowledge or constructive knowledge of the activities of the non-state actors. The Court held that indirect evidence may be used to prove knowledge and that knowledge may be "inferred from facts provided they leave no room for reasonable doubt". The court was clear, however, that the mere fact that control is exercised by a state over its territory is not reason, of itself, to impute knowledge of an unlawful act perpetrated therein (1949 ICJ 4, p. 18).

The principle can be illustrated by reference to the ransomware attack on the Health Service Executive (HSE) on 14 May 2021. The attack caused severe and significant disruption and the HSE estimated that 80% of its electronic health records were encrypted (PwC, 2021, p. 15). Despite receiving the decryption key on 20 May 2021, it took until 14 September 2021 to decrypt all the servers (PwC, 2021, p. 4). Irish media outlets, including RTÉ and the Irish Times, alleged that the attack was carried out by a criminal organisation called *Wizard Spider*, which is based in St Petersburg (Reynolds, 2021; Gallagher, 2021). This claim was repeated by the CCD COE (2021). The cyberattack was certainly a breach of sovereignty and, therefore, an international wrong. It also had serious adverse consequences for the Irish State and so this part of the test is met. The issue of Russia's knowledge of the activities of *Wizard Spider* is more difficult to address. Russia has been criticised widely for not doing enough to prevent cyberoperations from its territory (see for example; Corera, 2021; Khurshudyan & Morris, 2021) and is accused of using cyberoperations to undermine the health services of Western governments for strategic gain (Corn, 2020, p. 5). As outlined, there is insufficient state practise to determine whether these facts would be sufficient to impute constructive knowledge of the activities of *Wizard Spider* to the Russian State. It seems likely that proof of knowledge, even by indirect means as outlined in the *Corfu Channel Case*, would not be met. The lack of consensus on the nature of the principle, together with the uncertainty as to what constitutes a breach of it, and the difficulties of imputing knowledge, illustrate the impediments to applying this principle in practise.

The principles analysed above highlight the difficulties of applying international law in cyberspace; a "strategic environment for which it is misaligned" (Fischerkeller, 2021). International law evolved in response to the conventional kinetic environment, in which strategic advantage is gained by force or the threat of force. In cyberspace, strategic advantage is achieved by the exploitation of vulnerabilities and contest below the threshold of *jus ad bellum*. It is unsurprising, therefore, that international law struggles to apply neatly to sub-threshold cyber-contest. These principles are, however, not without utility. States have been willing to call out breaches of sovereignty in cyberspace and to make attributions against malicious state cyberoperations. With further development and agreement, the principle of non-intervention can ground lawful responses to foreign interference, deception, election meddling, and information conflict. The principle of due diligence creates a duty of care towards other states and can be used even when physical harm does not arise. As illustrated, contestation and uncertainty remain regarding its practical implementation, however, there is potential for international law to regulate state behaviour. The *Voluntary National Contributions* are a foundation upon which states can build to improve the application of international law in

cyberspace. The successful governance of cyberspace depends, however, on states continuing to engage to build on that foundation.

Addressing the Deficits in International Law

Non-Binding Norms

The points of divergence between states on principles of international law, perhaps, create a gap in which norms can set the benchmark for acceptable state behaviour. Norms differ from international law in that they are explicitly non-binding and breaches do not give rise to international legal responsibility. The 2015 UN GGE report outlined eleven non-binding norms that have since been adopted by the General Assembly. The report specifies that "norms reflect the expectations of the international community [and] set standards for responsible State behaviour…" (UN, 2015). Tikk argues that the use of norms by states must be monitored to determine if they are, indeed, intended to promote better state behaviour in cyberspace, or whether they are a means of circumventing international law (2020, p. 15). The report of the UN OEWG in 2021 explicitly stated that norms do not replace international law and "[n]orms do not seek to limit or prohibit action that is otherwise consistent with international law" (UN, 2021b, p. 5). The use of norms can, perhaps, be seen as an attempt to achieve international consensus on advancing cooperation in cyberspace, without confronting the harsh realities of conflicting political, diplomatic, and strategic interpretations of international law. Non-binding norms allow states to engage, however, the cost of that engagement is uncertainty regarding the rights and obligations of states until states reclaim their central role as lawmakers in the international domain. Mačák, however, uses the analogy of the development of legal regulation in the Antarctic where non-binding norms paved the way for consolidation into 'hard law' (2017, p. 893). Similarly, the first international conventions on nuclear safety adopted the non-binding standards that had developed in the previous decades (Mačák, 2017, p. 893). In the absence of agreement, norms have the potential to be a foundation on which agreement is based and, with time, can evolve into accepted standards of state behaviour. The utility of norms will be explored more fully in Part Three.

A Treaty for Cyberspace

Given the difficulties of applying international law in cyberspace, it might be concluded that a new instrument of international law is necessary for cyberspace. The principle of *lex specialis derogat legi generali* determines that specific law will prevail over general law (International Law Commission, 2001, Art. 55). A convention could provide an agreed framework, within which the international community could address cyberthreats, ensure the consistent application of international law, and prevent conflict. A treaty offers the potential to overcome the uncertainties and gaps that exist in relation to international law in cyberspace.

Proponents argue that the development of an international treaty pertaining to cyberoperations could provide clarity on matters such as determining a breach of sovereignty, attribution of state responsibility, and the setting of evidentiary standards for attribution. Russia advocates that an international convention is necessary to govern cyberspace, while China also does not rule out the necessity of developing a treaty to address the shortfalls in international law (Delerue, Douzet, & Gery, 2020, p. 41). Kettemann argues that an international treaty is the

most promising approach for ensuring binding law and outlines how the *Framework Convention on Climate Change* demonstrates that treaties can be concluded on complex topics (2017, p. 289). Equally, the *UN Convention on the Law of the Sea* and the *Outer Space Treaty* illustrate the potential for international agreement in contested domains.

Those against a treaty argue that it has unrealistic prospects of success and that it would constitute an attempt to control information and to infringe human rights (Burton, 2013; Maçák, 2017). Delerue states that cyberspace is a notional environment that "does not constitute a new domain or area of human activity for the purpose of international law" (2019, p. 303). Consequently, he believes that comparisons to specific regimes of international law that govern conventional domains are not useful. Geopolitical division is also manifest in relation to the debate on the need for a cyber treaty. The focus in Western and democratic states has been on the protection of a global and open internet (European Commission, 2020, p. 4; NATO StratCom, 2021), while states such as Russia and China are more concerned with controlling the information being carried across networks (Healey, 2011; Tan, 2020, p. 161). Maçák argues that Russian and Chinese proposals for internationally binding treaties have not been met with enthusiasm as they are seen as an attempt to control information and underpin authoritarian regimes (2016). In a submission to the UN OEWG, the EU stated that "[a] truly universal cyber security framework can only be grounded in existing international law…we neither call for, nor see the necessity for the creation of new international legal instruments for cyber issues" (EU Statement, 2019, p. 3). Similarly, many of the *Voluntary National Contributions* to the UN (for example, Estonia, Germany, Norway, Brazil) stress that international law provides a solid normative framework for state actions, regardless of the medium in which those actions occur (UN, 2021).

In the absence of unified political will, it is unlikely that a cyber treaty is possible. Geopolitical divisions are likely to further entrench positions and erode the appetite for compromise that would be necessary to achieve a treaty. A treaty might, furthermore, undermine efforts to practically apply existing international law to cyberoperations and cast doubt on that applicability. The statements in support of the sufficiency of existing international law indicate that states do not acknowledge a significant or insurmountable gap in the regulation of cyberoperations. Of course, such a position may be optimistic and geopolitical considerations are manifest in state positions on a cyber treaty. While much work remains outstanding, it appears that many states believe that existing international law can provide a universal framework for regulating cyberoperations, but if that is to be the case, they must work to develop a clear and shared understanding of its principles.

Conclusion

This Part addressed specific principles of international law and their applicability to sub-threshold cyberoperations. It found that while the *Voluntary National Contributions* are an important step in the development of *opinio juris*, they remain occasionally vague and often contradictory or conflicting, thereby challenging the ability of international law to provide a system that can regulate state behaviour in cyberspace. International law can set the boundaries for cyber-contest below the threshold of armed conflict, but states must move beyond generalities and be clear about what constitutes unlawful behaviour in cyberspace. The potential of norms to supplement principles of international law was addressed. While norms cannot supplant international law principles, they can contribute to achieving consensus on them and to setting

standards of acceptable state behaviour that may crystallise into hard law. The potential for a cyber treaty was also considered and it was concluded that, while a treaty might provide clarity on aspects of international law principles in cyberspace, it could potentially undermine efforts to interpret and apply existing international law.

Thus far the paper has sought to identify the strategic deficit in the regulation of sub-threshold cyberoperations caused by the problematic application of international law that results from its evolution in the conventional strategic environment and its geopolitical contestation. This Part illustrates this by reference to specific principles of international law but finds that international law principles have the potential to regulate cyberoperations. While it is imperfect and it is challenged by the geopolitical environment, the international law of cyberoperations could be seen to be in a development phase, as illustrated by the reliance on non-binding norms. With the continued commitment of states, it has the potential to offer better regulation of state activities in cyberspace. Part Three will place international law and cyberoperations in the context of small state security paradigms and consider the implications for the Irish State.

Part Three: Irish Cybersecurity and International Law

Part Three will examine Irish cybersecurity challenges with a particular emphasis on the role of international law in enhancing cybersecurity. Drawing on elements of small state security literature and cyber deterrence theory, Part Three is divided into three sections. Section one will consider the role of international law in enhancing cybersecurity. Section two will consider the nature of the cyberthreat that Ireland faces and place that threat in the context of geostrategic rivalry. Section three will apply theories of small state security and cyber deterrence to Irish cybersecurity.

Cybersecurity and International Law

Cyber threats are not restricted by borders and, as states are increasingly interconnected, it could be argued that all states, large and small, face similar cybersecurity challenges. The challenges are, however, exacerbated for small states as they often lack the resources, the personnel, and the specialised expertise of more powerful states. While it is recognised, therefore, that in today's connected world, security challenges are inextricably linked, it is argued that distinct security challenges remain for small states. Burton identifies three main conceptual models of small state security. These are alliance building, engagement in multilateral institutions, and the promotion of norms (2013, p. 217). This section analyses the role of international law in contributing to these security models and its role in furthering cyber deterrence.

Small State Security Models

The alliance building approach aligns with a Realist view of international relations. Small states seek alliances with more powerful states to ensure their security. The importance of military alliances in ensuring security is evident, however, collective security alliances are more difficult to implement in cyberspace, where sovereignty is ill-defined, attribution is complex, and there is uncertainty regarding what constitutes a use of force or an armed attack. The paradigmatic example is the Russia-linked cyberattack on Estonia in 2007. The attack illustrated the characteristics that have become the hallmarks of cyber-contest that we experience today;

plausible deniability, the use of cyber-proxies and sub-threshold cyberoperations. It further demonstrated that mutual defence clauses may struggle to guarantee the protection of sovereignty in cyberspace (Herzog, 2011, p. 56). Although collective alliances may not adequately tackle cyberoperations, organisations such as NATO continue to provide resources and support that can enhance cybersecurity. The CCD COE, for example, provides interdisciplinary expertise and training in cybersecurity through cooperation on technology, strategy, operations, and law.

Liberalism considers that states are rational actors that will seek mutual solutions to problems through international cooperation (Shehu & Leka, 2020, p. 202). The institutional model of small state security promotes the development of international institutions and encourages cooperative approaches to international security issues (Burton, 2013, p. 219). Keohane suggests that small and middle powers promote international institutions as they realise that, while they can do little together, they can do nothing separately (1969, p. 296). As outlined by the former New Zealand Permanent Representative to the UN, "[t]he obvious imbalance between small states and larger powers...means that multilateral systems based on the rule of law are vitally important for those smaller states, as they prevent that imbalance being used to their disadvantage" (McLay, 2011, cited in Lupel & Mälksoo, 2019, p. 2). Small states, therefore, have an interest in protecting a multilateral and rules-based international order. The initiatives by the UN to advance acceptable standards of state behaviour in cyberspace through the UN OEWG and the UN GGE are illustrative of the importance of institutionalism to cybersecurity. The effectiveness of these initiatives is hampered, however, by the divisive geopolitical environment. Burton points out that the UN Security Council did not debate the Estonian cyberattack, the cyberattacks on Georgia in 2008, or the *Stuxnet* attack against Iran (2013, p. 222), illustrating the limits of effective multilateralism in cyberspace.

Constructivist international relations theory argues that normative considerations are key factors in determining the actions of international organisations. Constructivism views state relationships as being based on norms, identity, and ideas (Beach, 2012, p. 19; Shehu & Leka, 2020, p. 202). Small states do not have the necessary military and economic power to influence world events and, accordingly, promote acceptable and stable standards of behaviour. Rothstein concludes that small states favour international organisations, not because they can protect the small state's security, but because the international organisation allows small states to work collectively to develop international attitudes and norms that shape a favourable international culture (1968, p. 29, cited in Keohane, 1969, p. 294). Tan believes that small states must be proactive in participating in norms discussions to create a "rules-based order for cyberspace…lest larger states run roughshod over the interests of smaller states in cyberspace" (2020, p. 169). Small states, thus, can benefit both from the normative strength of international institutions and the balancing of power offered by them. As with institutionalism, normative security is hampered by geopolitics and, while normative values may influence international organisations, the interests of the powerful still matter greatly. Therefore, even though both institutionalism and norm development can contribute to cybersecurity, the divisive geopolitical situation must be recognised as a limitation on their effectiveness.

Cyber Deterrence

Some writers are sceptical of the possibility of deterrence in cyberspace. Libicki argues that "attribution, predictable responses, the ability to continue attacks, and the lack of a counterforce

option are all significant barriers" (2009). Fisherkeller and Harknett also believe that the uncertainties surrounding sovereignty in cyberspace, as well as competition characterised by constant contact mean that deterrence is simply not a credible strategy in cyberspace (2017, p. 382, p. 385).

Others suggest that deterrence can be a means of achieving strategic success in cyberspace. Healey points out that deterrence is operative as states have avoided attacks above the *jus ad bellum* threshold by seeking strategic advantage through competition short of armed conflict (2019, p. 4). Nye suggests a role for deterrence by norms and states that the multilateralisation of norms helps to raise the reputation costs of breaches (2017, p. 62). Kristiansen and Hoem also argue that a stronger normative framework for behaviour in cyberspace could prove capable of generating deterrence by norms and, potentially, provide an objective basis to legitimise deterrence by punishment (2022, p. 27).

Cyberspace is characterised by constant contact so it is recognised that deterrence can never achieve zero attacks, as is the goal of conventional or nuclear deterrence. Norms and principles of international law can, however, raise the cost calculation for cyberattacks and contribute to deterring state actions outside of agreed norms of behaviour. Deterrence can include denial through resilience, hardening of systems and capacity building, however, it must also include deterrence through specified actions in response to breaches of acceptable state conduct. This requires clear signalling what the cost for failure to comply entails. Disagreement on the applicable principles creates legal uncertainty regarding responses. States must, therefore, be clear what a breach of sovereignty, due diligence or non-intervention is in cyberspace and what cost will be imposed for that breach.

Applying International Law to Security Models

Small states can utilise international institutions to promote international law and norm development to encourage more stable international behaviour. Finnemore and Sikkink detail the emergence of norms in three stages; norm emergence, broad norm acceptance, and internationalisation (1998, cited by Crandall & Allan, 2015, p. 348). Norm entrepreneurs are needed to develop norms and to publicise them internationally. For example, after the 2007 cyberattack, Estonia became a leading proponent of enhanced cybersecurity. It became the location for NATO's CCD COE and has actively advocated for international cooperation, the promotion of international law, and the development of norms through organisations including NATO, the EU, and the UN (Crandall, 2014, p. 37). Part Two outlined that the international community is falling back on norms in a bid to achieve consensus on international law in cyberspace and, as great powers remain divided, small states can influence the development of these norms. Goetschel suggests that neutral states are particularly effective norm builders as they have a history of promoting soft power and of advocating for peaceful resolutions of conflict (Goetschel, 2011, p. 326). Success may be dependent on great power cooperation, but small states have a role to play (Burton, 2013, p. 237).

A response to cyberoperations premised on international law attracts legitimacy and can generate collective international support, leading to enhanced adherence to international law and norms. Aiesi and Minikus (2020), in considering conventional deterrence against Iran, find that "clear and explicit use of international law language would signal to adversaries the basis for

escalatory responses while simultaneously conveying the legality and legitimacy of a threatened use of force". Moynihan points out, however, that, while coordinated international action in response to cyberoperations utilises the "normative force of international law, it is notable that in each case the statements are vague about precisely which international rules are at issue, referring to 'international law' in general, or to 'norms' of responsible state behaviour" (2021, p. 398). This ambiguity and lack of clarity impedes the use of international law to impose a cost expectation and to contribute to deterrence by norms. The absence of agreement on international law in cyberspace as outlined in Part Two, suggests that deterrence is weak and normative pressure to conform to international law is diminished. To remedy this, states must set clear boundaries on acceptable behaviour by using the language of international law in response to cyberoperations.

The achievement of consensus and clarity on standards of acceptable behaviour is threatened by the contestation of foundational principles of international law, often along geopolitical lines. In 2016, China and Russia issued a joint declaration that highlights the disagreement between the West and East on fundamental principles of international law in cyberspace, including on sovereignty, non-intervention, and the applicability of human rights law (Mälksoo, 2016; Russia-China Declaration, 25 June 2016). Mälksoo describes the *Declaration* "as part of a struggle for ideational power and moral high ground regarding international law as the common language of the international community" (2016). Delerue believes that the divergent positions create "a risk of geographical fragmentation of international law norms applicable to cyberspace" (2019, p. 297).

The extent to which Russia's war against Ukraine has altered the threat landscape remains to be seen, but it signals an actualisation of the fissure between East and West, and it may hasten attempts by Russia and China to shape global governance and to promote their values and interests. The strength of international law is in its universality and, in the absence of agreement by all states, its application to cyberoperations will be tested. The geopolitical divide makes consensus on the application of international law in cyberspace problematic and the codification of norms and rules of international law on cyberoperations less likely. It can be argued that the normative force of international law is only effective when behaviour can be influenced by the imposition of costs, or by ideational factors, including diplomatic pressure or the risk of reputational or political consequences. It is less effective against states that feel that there is nothing to lose by violating rules and norms of international law (Tan, 2020, p. 162). Russia's actions have made it a pariah state, and one, potentially, that no longer runs the risk of losing reputation or political capital by not abiding by international law. In China's case, this is less so, however, disputes surrounding its actions in the South China Seas, its human rights record, and its approach to Taiwan are isolating it.

It is recognised that international law is being challenged by uncertainty and by contestation surrounding its principles and, *a fortiori*, by geopolitical tensions that are exacerbating uncertainty, increasing ideational competition, and diminishing the normative force of international law. It is argued, however, that international law can contribute to more stable and predictable state behaviour and can support models of small state security. Despite its difficulties, states continue to call on international law in response to cyberoperations, signalling the centrality of international law to legitimate state actions. While states may not invoke specific legal principles in attributing cyberattacks, they "do at least invoke the international legal order

and the norms of responsible behaviour…" (Delerue, Douzet, & Gery, 2020, p. 46). Furthermore, despite deep ideological differences during the Cold War, there was widespread agreement on the basic features of international law (Krieger & Nolte, 2019, p. 5). There is now broad agreement on the need to enhance security and guarantee stability in cyberspace and that desire can lead to agreement on standards of state behaviour in cyberspace, despite the geopolitical divide. Rajput argues that, while there is a risk of fragmentation of international law, the BRICS states are likely to attempt to shape international law in accordance with their priorities, while continuously participating in the existing structures (2019, 123). Therefore, while power is fragmenting from the traditional European/Western locus that was formerly the driving force of international law, this may have the effect of increasing the legitimacy of international law through greater global participation, rather than undermining it.

As argued by Hart (2012) and Henkin (1979), international law gives rise to meaningful obligations and, while there are breaches, violations can occur without undermining the validity of that law. The difficulty in relation to the international law of cyberoperations is that the breaches could be seen to be a more systematic lack of compliance, given the scale and intensity of state involvement in malicious cyberoperations. This sense of non-compliance may be driven by the uncertain application of international law principles in cyberspace. If the international law of cyberoperations is to be effective, states must engage, clarify their positions, and use its principles in response to cyberoperations. While the current geopolitical conditions make engagement more difficult, it is arguably even more crucial to continue to engage with all states on the application of international law in cyberspace to reduce volatility and uncertainty.

Mačák argues that instead of lamenting the crises of international law, it is more appropriate to view the current situation as an intermediate stage in the generation of 'hard law', as occurred during early attempts to regulate nuclear activities and the use of the Antarctic (2017, p. 894). The threat is broad and complex, and it will not be a straightforward process, however, states have taken a useful first step in identifying their national positions on international law in cyberspace and in agreeing norms of behaviour. Norms cannot replace international law, but they can complement and support it while the foundations of the international law of cyberoperations are crystallising through state dialogue and interaction. Mačák believes that the mix of soft law, combined with a growing set of binding rules "can provide a logical and functioning response to a novel phenomenon" (2017, p. 899). That international law is not a panacea is clear, however, states, through organisations such as the EU and the UN, can work towards developing a shared understanding of international law in cyberspace to prevent its fragmentation and enhance its applicability. Processes at international and regional levels enable dialogue and shape perceptions of accepted state behaviour that can then have a normative pressure. It is encouraging that the disagreement is not that international law applies in cyberspace or that it is binding, but rather the debate is focused on the interpretation of that law. The debate and disagreements can serve to underline the role of international law in the peaceful resolution of differences. While it appears that states can currently compete without restriction in cyberspace, multilateral processes are working towards shaping the parameters of that contest.

Cybersecurity in Ireland

The *National Cyber Security Strategy* defines cybersecurity as "the means of ensuring the confidentiality, integrity, authenticity and availability of networks, devices and data", however, it goes on to note that, as systems "have become more embedded and complex, securing these becomes simultaneously more important and difficult" (NCSC, 2019, p. 3). Ireland's security challenges are closely linked with the global cybersecurity environment and the *White Paper on Defence Update 2019* recognises a "blurring of the lines between inter-state conflict, terrorism and criminal activity, particularly in the cyber domain" (2019, p. 13). The *White Paper Update* concludes that "the complex and dynamic nature of security threats, vulnerabilities, and consequences in the cyber sphere are becoming increasingly clear – risks arise without regard for geography and in ways that challenge the ability of states to detect and respond appropriately" (Department of Defence, 2019, p. 15). The EU notes that interconnection is increasingly conflictual, and that cyberspace has become a field for strategic competition (Council of the EU, 2022, p. 2, p. 12). These documents illustrate a recognition of strategic competition in and through cyberspace that compounds the complexity of cybersecurity.

Ireland ranks fifth in terms of overall levels of digitisation in the EU (European Commission, 2021, p. 19) and the National Cyber Security Centre (NCSC) estimates that Ireland is home to more than 30% of the EU's data (NCSC, 2019, p. 8). Ireland is the location of major information technology (IT) companies, data centres and the headquarters of many multinational companies. Healey notes that "[a]s cyberspace becomes more existential for more states, the stakes continue to rise, elevating the risks along with them" (2019, p. 8). Ireland, thus, has a significant technological footprint, and its connectivity and technological dependence has "created a complex and evolving set of risks" (NCSC, 2019, p. 3). Ireland is vulnerable to cyberoperations and, furthermore, the consequences of those cyberoperations could have disproportionate effects. A focus solely on physical security and a reliance on geographical isolation can, therefore, no longer be the answer to Ireland's security.

The threat is amplified by geopolitical tensions in a shifting and emerging world order. Heinl (2019) suggests that revisionist states are utilising the potential of cyberoperations to change the world order in pursuit of their national interests. The recently released *Strategic Compass* recognises that we "face a competition of governance systems accompanied by a real battle of narratives" (Council of the EU, 2022, p. 7) and the EU's *Cyber Security Strategy* acknowledges that "[c]yberspace is increasingly exploited for political and ideological purposes, and increased polarisation at international level is hindering effective multilateralism" (European Commission, 2020, p. 2). While Ireland is vulnerable due to its connectivity, that vulnerability is compounded by geopolitical competition. Adversary states and their proxies are utilising cyberoperations to undermine democratic institutions, to sow division in societies, and to shape the contested geostrategic environment. The EU has previously highlighted potential Russian interference in French, German and Spanish elections (European Parliament, 2019). The Centre for Strategic and International Studies also points to Russian interference in Scotland's independence referendum, the Polish and Finnish elections in 2015, the 2016 Brexit vote, and in elections in France, Italy, Netherlands, the Czech Republic, and Spain in 2017 and 2018 (Tennis, 2020). These interventions sow disinformation and stoke divisions and Ireland cannot consider itself immune.

Applying Cybersecurity Theories to the Irish Context

In response to the challenges it faces, Ireland's *National Cyber Security Strategy* sets out a broad range of responses to reduce vulnerability and to enhance resilience (NCSC, 2019). The international dimension is recognised, both in terms of internet governance and in the importance of the diplomatic sphere (NCSC, 2019, p. 5). Measures identified include using cyber attachés and engaging in international organisations such as the CCD COE. Ireland cannot disengage from persistent strategic competition through either neutrality or geography and, in addition to the measures identified, the promotion of international law and norms through broader international institutional cooperation would provide a further means to enhance Irish cybersecurity.

Ireland is a professed multilateral state that is constitutionally committed to upholding international law (Bunreacht na hÉireann, 1937, Art. 29.3). This commitment is both a matter of interests and values. Former Minister for Foreign Affairs, Simon Coveney states that "Ireland depends on international law and a values-based, strong multilateral system to uphold our own sovereignty" (2021). Ireland can leverage its neutral status to foster international consensus and dialogue on cybersecurity. As suggested by Goetschel, neutrality is no longer seen as a means of ensuring security and it now carries a more normative utility. He believes that neutral states have a "comparative advantage in brokering new ideas in international relations" and they "are well positioned to further advance international norms in highly contested areas of international relations" (2011, p. 313).

As norms in the cyberdomain remain slow to develop, international law does not fit easily with advancements in cyberoperations. States that are engaged in offensive cyberoperations benefit most from the absence of international law in cyberspace and they are unlikely to promote its development. Strengthening the rules-based order and the multilateral system is in Ireland's interests as a small and globally connected state. Ireland can, therefore, contribute to the development of international governance through its role in multilateral organisations. Ireland has committed to setting out its position on the international law of cyberoperations and, by making its position clear and by responding on that basis, it can enhance deterrence and improve cybersecurity.

The contestation and politicisation of international law illustrates the weaknesses of relying on international law alone as a tool. Conversely international law continues to be at the centre of international pronouncements calling out unacceptable state behaviour. This illustrates the dichotomy at the heart of international law; a desire for a stable and predictable means of regulating state interactions, coupled with a temptation to manipulate, redefine, and violate its terms, particularly by great powers. Small states cling to international law as they understand that their security cannot be guaranteed by power alone and that the multilateral world order and acceptable norm development moderate great power dominance. While international law is challenged, both by an undermining of the rules-based world order and by the difficulty of applying it to cyberspace, small states have a vital interest in underpinning its primacy. International law in cyberspace is imperfect, however, the complexity and global effects of cyberattacks demand international cooperation.

CONCLUSION

Harknett and Goldman advocate seeing cybersecurity, not as a problem of technology, but as a "behavioral, policy, and strategic challenge in a technically fluid environment", thus requiring a comprehensive approach across many disciplines (2016, p. 83). That view is accepted and, accordingly, this paper examined the use of international law to regulate state behaviour in cyberspace and to enhance Irish cybersecurity as one part of the comprehensive approach. By analysing the application of international law to cyberoperations below the *jus ad bellum* threshold, this paper has shown that cyberspace is a complex and challenging environment for international law. It also argues that, while international law is not fully aligned to the manner in which cyber-contest has developed and international law cannot guarantee compliance, it can increase the costs for states that breach it and its principles are applicable. The utility of international law in cyberspace is, however, undermined by the fact that state positions often remain unclear, and states do not use the language of international law in response to cyberoperations. This remains an area that states should address and develop to improve adherence to agreed standards of behaviour in cyberspace.

Part One outlined that the fundamental characteristics of cyberoperations include persistent engagement and competition below the threshold of *jus ad bellum*. These characteristics result both from the structure of cyberspace and because of the potential to achieve strategic gain through constant sub-threshold cyber-campaigns. While cyber is an inherent part of the projection of military force above the *jus ad bellum* threhsold, state activities in cyberspace indicate the use of cyberoperations as a strategic alternative to armed conflict. The ubiquity of entry points, the relatively low cost of entry, the private control of much of the cyberspace architecture and the potential to achieve strategic advantage, incentivise the use of cyber-campaigns short of armed conflict. Persistent grey zone cyberoperations can be carried out and can advance a state's interests while undermining rival political systems without a serious risk of an escalation to armed conflict. Cyberoperations are inherently targeted at exploiting vulnerabilites, which may be societal or technological. Accordingly, international law has not proved fully capable of controlling state activities in cyberspace as it evolved to govern the use of kinetic force in the conventional strategic environment.

International law is further challenged by the geostrategic environment and by a challenge to the rules-based international order, with support for multilateralism and the rule of law apparently being undermined. The changing global balance of power towards new and emerging states suggests a challenge to the, hitherto often Western, interpretation of international law and states are using international law as a weapon of contestation. It is argued, however, that international law remains a normative force in regulating state behaviour and that states seek legitimacy through its use. It provides a common basis for interactions between states and, while it is threatened, breaches of international law are insufficiently common to destroy the sense of obligation that it imposes.

Part Two argued that international law is challenged in its application to cyberoperations as its principles are established slowly and through state practise over decades, while cyberoperations develop and evolve quickly as technology advances. This was illustrated by considering the principles of international law that are applicable to sub-threshold cyberoperations including sovereignty, due diligence, non-intervention, and the principle of state

responsibility. The application of these principles in cyberspace is difficult but, notwithstanding, states have been willing to use these principles in response to cyberoperations. To be more effective, however, states must clearly set out their positions on the international law of cyberoperations. The *Voluntary National Contributions* provide a useful starting point in identifying areas of agreement and divergence, however, that agreement is at an early stage. In the absence of consensus on the application of international law, states have relied on non-binding norms. While these are explicitly non-binding, they can set common standards of behaviour that, over time, can crystallise into *opinio juris*. The potential to develop a treaty on cyberspace was also considered and it was concluded that, while a treaty may provide clarity on aspects of international law, there is competition along geopolitical lines on what the purpose and outcome of such a treaty might be. There is, as it stands, insufficient political will to make a cyber treaty possible and states prefer to try to shape existing international law to cyberoperations. This may, in itself, be positive as it indicates a willingness to apply and use international law and it further underpins the centrality of existing international law.

Part Three analysed models of small state security and considered their applicability to cyberoperations. It argued that international law can contribute to institutionalist and normative models of small state security and to cyber deterrence, while recognising that geopolitical competition and the failure to use international law in response to cyberattacks is hampering that effectiveness. Part Three then considered Irish cybersecurity and illustrated the vulnerability that Ireland faces due to its levels of digitalisation and connectedness. It outlined how Ireland's vulnerabilities are compounded by geopolitical tensions and by ongoing competition to shape the emerging world order. Part Three also considered Ireland's use of international law to contribute to normative and institutionalist models of small state security and to enhance cyber-deterrence by norms. It concluded that, although international law is challenged, both by an undermining of the rules-based world order and by the difficulty of applying it to cyberspace, small states are likely to promote international law as they cannot rely on military power alone for security. To be effective, however, international law must be applied more clearly in response to cyberoperations. Ireland, as a small, neutral, and professed multilateralist state, is well placed to promote the development of international law and norms in cyberspace.

This paper asks whether international law can provide a means for the Irish State to regulate sub-threshold cyberoperations. The answer to this question, by necessity, draws on aspects of international law, legal theory, international relations theory, and security studies. While it attempts to provide a comprehensive analysis, the breadth of this paper is recognised as a limitation, and all the issues elucidated are worthy of more in-depth study. Space permitting, more attention would also be given to retorsion and countermeasures in response to cyberoperations.

This paper shows that, because of the global nature of the cyber-threat and the complexity that it poses, international cooperation is necessary. International law is facing a challenging period, if not a crisis, however, it retains its normative strength and remains central to international interactions. In cyberspace, however, international law principles and norms have not been fully established. While it is generally agreed that international law applies to cyberspace, how it should apply remains contested and state practice has not evolved to meet the quickly growing threat posed by cyberoperations. Small states rely on multilateralism and the rule of law to redress the balance of power in their favour, and they utilise international law and

norms to create more favourable international conditions. To be effective in cyberspace, however, more clarity is needed on the practical application of international law principles.

Cyberoperations are not just a continuum of the spectrum of military engagement. They are also a means of achieving strategic gain without the use of force and even as an alternative to war. In conventional domains, the actions of adversaries, their identities and their motivations are, generally, readily determined, monitored, and addressed. The same is not true in cyberspace where the problem of attribution makes the identity of adversaries and the nature of their activities difficult to pinpoint, and it is impossible to disengage from adversaries due to the interconnectedness of the environment. It is unsurprising that the traditional concepts of international law, centred on the use of force, armed attack, and based on the concept of sovereignty, struggle to adapt to the cyber-environment. Resultingly, there is difficulty in achieving agreement on the norms and rules of international law, which further incentivises sub-threshold cyberoperations. International law is constrained by its evolution to govern kinetic force in the face of the unique characteristics of cyberoperations.

The paper addresses the challenges facing international law and considers whether these result in the ubiquity of cyberoperations and a lack of regulation of cyberspace. Without the benefit of a longer view of history, it is not possible to say definitively whether international law is in the midst of a crisis, however, it is certainly in a challenging and unsettling period. States have shown a commitment to determining the international law of cyberoperations through their *Voluntary National Contributions*, however, and while there are disagreements on the details, this process sets the parameters for dialogue between states. International law can provide a framework for a structured and open debate that will advance international understanding of acceptable state behaviour in cyberspace. It may be correct to state that, currently, international law does not adequately regulate state behaviour in cyberspace, however, it has the potential to do so through iterative processes including the UN GGE and the UN OEWG. As outlined by Delerue *et al*, "international law remains a pillar of the international legal order, even with the need to define the rights and obligations of states in cyberspace" (2020, p. 59). International law on its own may not be sufficient, or even preferable, as a means of regulating state behaviour in cyberspace, but it is necessary as part of the comprehensive approach to tackling the threat posed by cyberoperations.

Please note that the views expressed in this article are those of the author alone and should not be taken to represent the views of the Irish Defence Forces, the Command and Staff School or any other group or organisation.

REFERENCES

Aiesi, M. J., & Minkus, A. (2020). *The US Should Communicate Jus ad Bellum Lexicon to Strengthen its Deterrence Posturing. Lawfare Blog*. Retrieved from https://www.lawfareblog.com/us-should-communicate-jus-ad-bellum-lexicon-strengthen-its-deterrence-posturing

Alperovitch, D., & Ward, I. (2021). *White House Responded to Chinese Hacks of the Microsoft Exchange Servers This Week. Is It Enough? Lawfare Blog*. Retrieved from https://www.lawfareblog.com/white-house-responded-chinese-hacks-microsoft-exchange-servers-week-it-enough

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming. *Comparative Strategy, 12* (1), 141 165.

Babbage, R. (2019). Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and how the West can Prevail. *Center For Strategic and Budgetary Assessments, 1*.

Banks, W. (2017). State Responsibility and Attribution of Cyber Intrusions After Tallin 2.0. *Texas Law Review, 95*(7), 1487 - 1513.

Beach, D. (2012). *Analyzing Foreign Policy.* New York: Palgrave Macmillan.

Borrell, J. (2021, September 24). *High Representative for the EU*. Retrieved from https://twitter.com/josepborrellf/status/1441382364391694337?lang=ar

Borrell, J. (2022). *Foreword to the Strategic Compass.* European External Action Agency. Brussels: Council of the EU. Retrieved from https://eeas.europa.eu/sites/default/files/foreword_-_a_strategic_compass_to_make_europe_a_security_provider.pdf

BRICS. (2017). *BRICS Leaders Xiamen Declaration.* Toronto: University of Toronto.

Bruneé, J. (2018). Multilateralism in Crises. *American Society of International Law*.

Bunreacht na hÉireann. (1937). *Bunreacht na hÉireann.* Irish Statute Book.

Burchardt, D. (2019), The Relationship between Legality and Legitimacy: A Double-Edged Sword. In G. Nolte, H. Krieger, & A. Zimmermann (Eds.), *The international rule of law: rise or decline?* (pp. 311-344). Oxford: Oxford University Press.

Burton, J. (2013). Small States and Cyber Security, The Case of New Zealand. *Political Science, 65*(2), 216-238.

Case Concerning Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*) 1986 ICJ 215.

CCD COE. (2021). *Ireland's Health Service Executive ransomware attack (2021)*. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Ireland%E2%80%99s_Health_Service_Executive_ransomware_attack_(2021)

Centre for Strategic & Interntaional Studies. (2021). *Significant Cyber Incidents*. Retrieved from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

CFR. (2010). *Stuxnet*. Retrieved from https://www.cfr.org/cyber-operations/stuxnet

Chircop, L. (2019). Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0. *Melbourne Journal of International Law, 20* (2).

Corera, G. (2021). *BBC News*. Retrieved from https://www.bbc.com/news/technology-57084943.

Corfu Channel (*UK v. Albania*) 1949 ICJ 4.

Corn, G. (2020). Cover Deception, Strategic Fraud, and the Rule of Prohibited Intervention. *Hoover Working Group on National Security, Technology and Law, Aegis Series Paper No. 2005*.

Corn, G., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL, 111*(207).

Council of the EU. (2020). *Council Implementing Regulation 2020/1125.* Brussels: Official Journal of the EU.

Council of the EU. (2022). *A Strategic Compass for Security and Defence 7371/22.* Brussels: EEAS.

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. *Defence Studies, 14*(1), 30-55.

Crandall, M., & Allan, C. (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy, 36*(2), 346-368.

Delerue, F. (2019). Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review, 52*(3), 295–326.

Delerue, F., Douzet, F., & Gery, A. (2020). *The geopolitical representations of international law in the international negotiations on the security and stability of cyberspace.* Paris: EU Cyber Direct.

Department of Defence. (2019). *White Paper on Defence Update 2019.* Dublin: Government of Ireland.

Director of National Intelligence. (2016, October 07). *Press Release Joint DHS ODNI Statement on Election Security.* Retrieved from https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1635-joint-dhs-and-odni-election-security-statement

Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practise. *The American Journal of Intenational Law, 112*(4), 583-657.

Efrony, D. (2021, July 16). *The UN Cyber Groups GGE and OEWG. A consensus is optimal but time is of the essence. Just Security.* Retrieved from https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/

EU Statement. (2019, September 09). *EU General Statement to the OEWG on Cyber.* Retrieved from https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/EU+General+Statement+to+the+OEWG+on+Cyber%2C+First+Session.pdf

European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade.* Brussels: European Commission.

European Commission. (2021). *Digital Economy and Society Index (DESI) 2021.* Brussels: European Commission.

European Parliament. (2019, November 21). *Europarl.* Retrieved from https://www.europarl.europa.eu/doceo/document/P-9-2019-003967_EN.html

Fischerkeller, M. (2021). *Current International Law is not an Adequate Regime in Cyberspace. Lawfare Blog.* Retrieved from https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace

Fischerkeller, M., & Harknett, R. (2017). Deterrence is Not a Credible Strategy for Cyberspace. *Orbis, 61*(3), 381-393.

Fischerkeller, M., & Harknett, R. (2018, May). Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation. *Institute for Defense Analyses*, pp. 1-29.

Fishcerkeller, M., & Harknett, R. (2020). Cyber Persistence, Intelligence Contests and Strategic Competition. *Texas National Security Review*.

Gallagher, C. (2021, May 22). *Give me a crash course in... the Wizard Spider cyber attack.* Retrieved from https://www.irishtimes.com/life-and-style/give-me-a-crash-course-in-the-wizard-spider-cyber-attack-1.4571382

Goetschel, L. (1998). The Foreign and Security Policy Interests of Small States. In L. Goetschel (Ed.), *Today's Europe: Small States Inside and Outside the European Union* (p. 28). Dordrecht: Kluwer.

Goetschel, L. (2011). Neutrals as Brokers of Peace Building Ideas? *Cooperation and Conflict, 46*(3), 312–33.

Harknett, R. (2018). *United States Cyber Command's new vision: what it entails and why it matters. Lawfare.* Retrieved from https://www.lawfareblog. com/united-states-cyber-commands-new-vision-what-it-entails-and-why- it-matters

Harnkett, R. (2019). *National Security Archive*. Retrieved from Cyberspace as a Strategic Environment: https://nsarchive.gwu.edu/news/cyber-vault/2019-11-26/cyberspace-strategic-environment

Harknett, R., & Goldman, E. (2016). The Search for Cyber Fundamentals. *Journal of Information Warfare, 15*(2), 81-88.

Harknett, R., & Smeets, M. (2020). Cyber Campaigns and Strategic Outcomes: The Other Means. *Journal of Strategic Studies*, https://doi.org/10.1080/01402390.2020.1732354.

Harland, S., & Hemsley, D. (2019). Persistent Engagement and Information Campaigning. *Defence Forces Review, 13*, 147-153.

Hart, H.L.A. (2012) *The Concept of Law* (3rd ed.). Oxford: Oxford University Press.

Hathaway, O. (2005) Between Power and Principle: An Integrated Theory of International Law, U*niversity of Chicago Law Review, 72*.

Henkin, L. (1979). *How Nations Behave: Law and Foreign Policy* (2nd ed.)(extract). New York: Columbia University. In Sassoli, M. & Bouvier A. (2006) *How does law protect in war? Cases, documents and teaching materials on contemporary practice in International Humanitarian Law* (2nd ed.) (pp. 91-99) Geneva: ICRC

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity, 5*(1), 1-15.

Heinl, C. (2019). Russia and China: Their Impact on Irish Security from a Cyber Perspective. *Wordpress*. Retrieved from https://caitrionaheinlcyberpolicywatch.wordpress.com/2019/05/30/russia-and-china-their-impact-on-irish-security-from-a-cyber-perspective/

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60.

International Law Commission. (2001). *Draft Articles on the Responsibility of States for Internationally Wrongful Acts.* New York: United Nations General Assembly Resolution 56/83.

Island of Palmas (*United States v Netherlands*), (1928) II RIAA 829.

Keohane, R. (1969). Lilliputians' Dilemmas: Small States in International Politics. *International Organisation, 23*(2), 291-310.

Kertzer, D. (1988). *Ritual, Politics and Power.* Yale: New Haven.

Kettemann, M. (2017). Ensuring Cybersecurity through International Law. *HeinOnline, 69*(2), 281.

Khurshudyan, I., & Morris, L. (2021). *Russia Ransomware Cybercrime*. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/europe/russia-ransomware-cyber-crime/2021/06/11/e159e486-c88f-11eb-8708-64991f2acf28_story.html

Koh, H. (2019). *The Trump Administration and International Law* (1 ed.). Oxford: Oxford University Press.

Krieger, H., & Nolte, G. (2019). The International Rule of Law—Rise or Decline?—Approaching Current Foundational Challenges. In G. Nolte, H. Krieger, & A. Zimmermann (Eds.), *The international rule of law: rise or decline?* (pp. 1-30). Oxford: Oxford University Press.

Kristiansen, M., & Hoem, N. (2022). Small players in a limitless domain: Cyber deterrence as small state strategy. *Comparative Strategy, 41*(1), 19-31.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica: Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/ monographs/2009/RAND_MG877.pdf
Liebetrau, T. (2022, February 04). *Cyber conflict short of war: a European strategic vacuum.* Retrieved from https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991

Lupel, A., & Mälksoo, L. (2019). A Necessary Voice: Small States, International Law, and the UN Security Council. *International Peace Institute*, 1-15.

Mälksoo, L. (2016). *Russia and China Challenge the Western Hegemony in the Interpretation of International Law. EJIL Talk*. Retrieved from https://www.ejiltalk.org/russia-and-china-challenge-the-western-hegemony-in-the-interpretation-of-international-law/

Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyberoperations by Non-State Actors. *JCSL, 21*, 405.

Mačák, K. (2017). From Cyber Norms to Cyber Rules: Re-engaging States as Lawmakers. *Leiden Journal of International Law, 30*(4), 877-899.

Microsoft. (2018). *Cybersecurity Policy Framework.* Microsoft.

Ministère des Armées. (2019). *International Law Applied to Operations in Cyberspace.* Paris: DICOD.

Ministry of Defence UK. (2015). *Future Operating Environment 2035.* London: Ministry of Defence.

Moynihan, H. (2019, December). *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. Chatam House.* Retrieved from https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Moynihan, H. (2021). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy, 6*(3), 394-410.

Mueller, R. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* Washington: US Department of Justice.

National Intelligence Council. (2021). *Foreign Threats to the 2020 US Federal Elections.* National Intelligence Council.

NATO StratCom. (2021). *Russia's Strategy in Cyberspace.* Riga: NATO StratCom COE and NATO Cooperative Cyber Defence COE.

NCSC. (2019). *National Cyber Security Strategy 2019 - 2024.* National Cyber Security Centre.

Nye, J. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly, 5*(4), 20.

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.

Office of the Director of National Intelligence. (2017). *Background to Assessing Russian Activities and Intentions in Recent US Elections.* Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Ponta, A. (2021). Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes. *American Society of International Law, 25*(14), 1-7.

PwC. (2021). *Conti cyber attack on the HSE Independent Post Incident Review.* Dublin: PwC (Commissioned by the HSE).

Rajput, A. (2019). The BRICS as 'Rising Powers' and the Development of International Law. In G. Nolte, H. Krieger, & A. Zimmermann (Eds.), *The international rule of law: rise or decline?* (pp. 105-125). Oxford: Oxford University Press.

Reynolds, P. (2021, May 19). *'Wizard Spider': Who are they and how do they operate?* Retrieved from https://www.rte.ie/news/crime/2021/0518/1222349-ransomware-crime-group/

Rid, T. (2013). *Cyberwar will not take place* (1 ed., Vol. 35). Oxford: Oxford University Press.

Russia-China Declaration. (25 June 2016). *The Ministry of Foreign Affairs of the Russian Federation, The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law*. Retrieved from https://archive.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2331698

Schmitt (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations.* Cambridge University Press.

Schmitt, M., & Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound, 111*, 213-218.

Shehu, S., & Leka, G. (2020). Small States Security Through International Integrations: A Theoretical Approach. *Justicia, 8*(13), 199-206.

Tan, E. (2018). Cyber Deterrence in Singapore. *RSIS Working Paper*.

Tan, E. (2020). *A Small State Perspective on the Evolving Nature of Cyber Conflict.* Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Tan_158-171.pdf

Tennis, M. (2020, July 20). *Russia ramps up global elections interference. Lessons for the United States. Centre for Strategic and International Studies.* Retrieved from https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states

Tikk, E. (2020). International Law in Cyberspace: Mind the gap. *EU Cyber Direct*.

Tsagourias, N. (2019). The Slow Process of Normativizing Cyberspace. *AJIL Unbound 113, 71-75.*

UK National Cyber Security Centre. (2022). *Russia DDOS Involvement in Ukraine. www.ncsc.gov.uk*. Retrieved from https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine

UN. (1945). *Charter of the United Nations.* New York: www.refworld.org/docid/3ae6b3930.

UN. (2013). *Group of Governmental Experts Report on Developments in the Field of ICT.* UN Doc A/68/98

UN. (2015). *Group of Governmental Experts Report on Developments in the Field of ICT.* UN Doc A/70/174.

UN. (2021). *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Expert.* New York: United Nations A76/136.

UN. (2021a) *Group of Governmental Experts Report on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. UN Doc A76/136

UN. (2021b). Open-ended working group on developments in the field of information and telecommunications in the context of international security. AC.290/2021/CRP.2.

United States v. Arjona (1887) 120 US 479
US Cyber Command. (2018). *Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command.* Washington: US Cyber Command.

Väljataga, A. (2018). *Tracing Opinio Juris in National Cyber Security Strategy Documents.* Tallinn: NATO Cyber Defence Centre of Excellence.

Wilt, H. v. (2019). State Practice as an Element of Customary International Law: A White Knight in International Criminal Law? *International Criminal Law Review, 20(5)*, 784-804.

Wouters, J. (2019). International Law, Informal Law-Making, and Global Governance in Times of Anti-Globalism and Populism. In G. Nolte, H. Krieger, & A. Zimmermann (Eds.), *The international rule of law: rise or decline?* (pp. 242-264). Oxford: Oxford University Press.

Wrange, J., & Bengtsson, R. (2019). Internal and external perceptions of small state security: the case of Estonia. *European Security, 28*(4), 449-472.