International Law in Cyberspace: Mind the gap

Eneken Tikk
Cyber Policy Institute
March 2020
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Abstract</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Key points</strong></td>
<td>2</td>
</tr>
<tr>
<td>1  Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2  What is international law?</td>
<td>4</td>
</tr>
<tr>
<td>3  What is responsible state behaviour</td>
<td>6</td>
</tr>
<tr>
<td>4  How does international law apply?</td>
<td>8</td>
</tr>
<tr>
<td>5  International cybersecurity issues</td>
<td>11</td>
</tr>
<tr>
<td>5.1 The state of cyberconflict</td>
<td>11</td>
</tr>
<tr>
<td>5.2 ICTs as a threat to international peace and security</td>
<td>12</td>
</tr>
<tr>
<td>5.3 Permissibility of cyber operations</td>
<td>14</td>
</tr>
<tr>
<td>6  The current discourse</td>
<td>15</td>
</tr>
<tr>
<td>6.1 National statements about international law and cyber governance</td>
<td>15</td>
</tr>
<tr>
<td>6.2 Submissions to the First Committee</td>
<td>17</td>
</tr>
<tr>
<td>6.3 Further views</td>
<td>21</td>
</tr>
<tr>
<td>6.4 Consequences of ‘bad behaviour’ in cyberspace</td>
<td>22</td>
</tr>
<tr>
<td>6.5 Scholarly debate</td>
<td>24</td>
</tr>
<tr>
<td>7  Have we been here before?</td>
<td>25</td>
</tr>
<tr>
<td>7.1 International regimes on the development and use of ICTs</td>
<td>25</td>
</tr>
<tr>
<td>7.2 Experience from earlier disarmament issues</td>
<td>27</td>
</tr>
<tr>
<td>7.3 Inquiries into further fields of (international) law</td>
<td>29</td>
</tr>
<tr>
<td>8  Conclusion</td>
<td>30</td>
</tr>
<tr>
<td><strong>About the author</strong></td>
<td>31</td>
</tr>
</tbody>
</table>
Acknowledgments

This paper builds on the discussion between the author and Russell Buchan, Antonio Coco, François Delerue, Talita de Souza Dias, Jean d’Aspremont, Helen Eenmaa-Dimitrieva, Duncan Hollis, Kristine Hovhannisyan, Mika Kerttunen, Jan Klabbers, Elaine Korzak, Martti Koskenniemi, Joanna Kulesza, Marja Lehto, Iulia Motoc, Patryk Pawlak, Mirva Salminen, Barrie Sander, Nicholas Tsagourias, Tobias Vestner, and Sean Watts during the International Law workshop held in Helsinki, Finland, on 27-28 September 2019. The author would also like to thank Aude Gery and Catherine Lotrionte, who provided comments on the earlier drafts of this paper. Any mistakes or omissions are those of the author alone.

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.
Abstract

It is a fundamentally European conviction that states’ actions in cyberspace as in any other domain, must be guided and governed by international law. However, as united as European states and scholars stand on this premise, they have demonstrably different views on what international law is and how to apply it. These differences can be (and have been) construed as an exploitable fault line in the European and wider Western liberal approach to international law. Yet, our differences should rather be seen as an opportunity to inform and enrich further discussions on how to sustain and promote lawful and responsible behaviour in ways that uphold and promote shared values and goals. This conviction serves as a common platform on which to invite, introduce, and debate views on how to best apply international law to issues of cybersecurity, since everyone joining this platform is interested in helping to advance international law - and improve international life. This paper calls for an open, transparent, inclusive, critical and continuous dialogue on how international law applies to state use of ICTs, building on best partnership efforts between governments and academia and increasing cooperation between European and non-European scholars.

Key points

> Promoting and fortifying international law is essential for sustaining ICTs as a technology of peace and prosperity.

> How international law is and will be applied to issues of cybersecurity depends on our ability to understand and convince each other about the benefits and downsides of particular views taken on international law.

> Different voices in the discussion about how international law can strengthen and diversify the debate, help to understand and reach wider constituencies, and engage and accommodate best practices of international law.

> An open, transparent, inclusive, critical and continuous debate on how international law applies to state use of ICTs should include and invite all stakeholders, including the private sector and users.
"A just, stable and peaceful digital order can be achieved only if it is based on international law. It is universally recognised that existing international law also applies to cyberspace. Further international cooperation in this field will benefit us all."¹

1 Introduction

It is a fundamentally European conviction that states’ actions in cyberspace (as in any other domain) must be guided and governed by international law. The European Union (EU) and individual Member States have firmly expressed the view that international law applies to states’ uses of information and communication technologies (ICTs). However, as united as European states and scholars stand on this premise, they have demonstrably different views on what international law is and how to apply it. These differences can be (and have been) construed as an exploitable fault line in the European and wider Western liberal approach to international law. Yet, these differences can also be seen as an opportunity to inform and enrich further discussions within the EU and like-minded states on how to sustain and promote lawful and responsible behaviour in ways that uphold and promote shared values and goals.

European conclusions and a common understanding can demonstrate to other states and scholars that the European way of interpreting and applying international law in cyberspace offers a solid basis for reflection and a constructive exchange.

The United Nations Group of Governmental Experts (UNGGE) and the UN Open-ended Working Group (OEWG) provide the EU and its Member States with an avenue for sharing their experience with international law. Here, European conclusions and a common understanding can demonstrate to other states and scholars that the European way of interpreting and applying international law in cyberspace offers a solid basis for reflection and a constructive exchange.

This paper builds on the author’s own conviction that, among those who unwaveringly agree that international law underpins state use of ICTs, differences of opinion about what international law is and how (or why) it should be applied constitute an opportunity to enrich and fortify the discourse. It is with this confidence that this paper follows the author’s quest for further views and contributions to frequently asked questions in international cybersecurity discussions: What is international law? How does it relate to the concept of responsible state behaviour? What do we mean when we claim that international law applies in cyberspace? What are the issues we trust or expect international law to solve? How can we improve a common understanding and an appreciation of international law?

The current discussion of international law is often limited to isolated claims about what particular rules and standards of international law have, or have not, been violated or how particular activities ought, or ought not, be conducted. In government-on-government dialogue, the discussion remains contoured by strong political interests and therefore lacks detail and theatre for compromise. Academic debates remain inconclusive in the absence of more detailed information, thus rendering an “it depends” outcome.

How international law is and will be applied to issues of cybersecurity depends on our ability to understand and convince each other about the benefits and downsides of particular views taken on international law. It is essential to understand how and why states and scholars regard certain uses of ICTs normal or problematic and which justifications they offer (and accept) to particular uses of ICTs. Broadening one’s perspectives of how international law may be understood or approached helps one understand and reach wider constituencies and engage and accommodate alternative views.

Building on interviews and discussions with numerous scholars and experts, this paper calls for a more critical and far more inclusive debate among all those who consider international law to be the highest authority in international relations and international life. The reader will be offered views as to why the question of international law and cyberspace is a timely one, why the propositions made about international law so far are anything but conclusive and why this topic requires and deserves European states’ and scholars’ continued attention and increased contribution.

2 What is international law?²

There are different ways to think about international law. A textbook approach would define it as a body of binding rules and principles for nation states.³ A dogmatic discussion of international law can therefore easily be limited to contradicting claims about the existence or non-existence, sufficiency or insufficiency, of such binding rules and principles. These doctrinal debates reveal the dualist nature of international law that fully permits “sovereignty” to co-occur with “subjection to law”, or that allows the prohibition of the use of force to coexist with the right of self-defence.

International law is frequently identified by where it can be found. As such, it manifests in international legal instruments and recurring state practice, legal arguments and reasoning. Article 38 of the Statute of the International Court of Justice (ICJ) guides the Court to international conventions, international custom, the general principles of law recognised by civilised nations, as well as judicial decisions and the teachings of the most highly qualified publicists of the various nations.

How international law is and will be applied to issues of cybersecurity depends on our ability to understand and convince each other about the benefits and downsides of particular views taken on international law. However, in the self-regulating international community, international law is more than mere doctrine and artefacts, though it can occasionally seem like less. Any one definition is not likely to reveal the role and full potential of international law in international life. If we limit our thinking about international law to particular rules and their contingent interpretations, we are doomed to be disappointed, confused and defensive - it becomes “our” international law against “theirs”.

Framing of “international law as …, instead of is …” helps to avoid the trap of exhaustive definitions and lists.⁴ International law can be thought of as a particular regulatory technique - the ability to draft and decipher rules and principles. In this embodiment, international law is about capturing the current and potential interests of states in legal texts. In such forms, international law is more principled than it is precise. Universal agreements, such as the UN Charter, are inclusive by membership yet inevitably cannot contain very precise or detailed instructions for behaviour. The law can be very particular when focused on narrow questions or when agreed upon by a small number of countries. When the latter is true, however, legal guidance remains limited in scope and coverage.

The relative vagueness of written international law that allows its rules and standards to be applied to a wide variety of situations also allows international law to be construed as lawfare - the use of law for

⁴ Martti Koskenniemi (2019).
International law manifests in competing arguments about its content, purpose, or context. This face of international law is hard to overlook as it becomes a tradecraft, reminiscent of Hermann Hesse’s *Glasurenspiel*, where the implementation of international law follows argumentation and logic that is only alluded to. Such arguments can be so sophisticated that they are not easy to conceive or relate to, or so obvious that their restatement implies a disguised objective. Following such arguments and positions well requires indoctrination in particular readings of international law or being privy to exclusive logic of its study and interpretation by particular states or schools.

International law can be thought of as the *jurisprudence* of international courts and tribunals. Indeed, this facet of international law becomes most detailed, and also most immediately binding, for states that decide to subject their differences to a particular legal procedure. However, the decisions of the ICJ and other courts have no binding force except between signatories, and even then, only within the scope of that particular case. Furthermore, such a conception of international law overlooks its routine functioning, i.e., the normalcies of international law that materialise in the smallest things like making a phone call abroad, traveling to another country, or sending an email.

International law is to be acknowledged as a means of communication, cooperation, and exchange of experience and visions on how to make international life better and to reduce friction in international relations. In this setting, we may detect the differences between scholars and states on particular issues, yet we take these disparities as an opportunity to study, clarify, and enhance this body of law. In this reading of international law, differences between scholars and governments are perceived and taken as honest ingredients for building a better and more solid foundation for international life.

This list can go on. International law can be thought of as an infrastructure of prosperity and certainty. For instance, the United Nations Convention of the Law of the Sea (UNCLOS) has brought important economic advances to coastal states while providing legal security and certainty to others, thus facilitating international cooperation and bringing benefits to participating states. The ”100 Ways” project of the American Society of International Law (ASIL) illustrates how international law brings benefits to everyday life.

Dismissing the existence of international law as a single or unified disciplinary object of study, or as a uniquely identifiable regime, Kennedy contends that international law is the messy, contradictory, and confused product of the work of thousands of international lawyers in their respective roles and on their respective projects. “International law is different in different places”, he further warns. Studies of the similarities and differences in international law must therefore focus not on mere words but on the underlying assumptions upon which different states and scholars rest their narratives and pleas.

It may be useful to think of international law as the sum of accountability, responsibility, and restraint that states have come to accept and exercise in their behaviour. International law is made up of the views, attitudes, and perceptions towards international affairs that states have held and deposited over

---

5 Article 59 of the Statute of the International Court of Justice.
8 David Kennedy (1999).
9 Ibid.
10 Ibid.
time, both individually and collectively. These views gradually settle into the normalcy of international life. As a result, whatever issues are highlighted by the current political differences or changes in the balance of power, their disruptiveness to international security and stability is diminished by the cumulative experience of past contestations and resolutions.

International law can be detected and observed everywhere. Complaints about the complexities and limits that ICTs impose on the applicability of international law are based on the assumption that international law governs, and ought to govern, the use of ICTs by states. International law becomes evident in justifications that states offer for their behaviour, as well as in their reactions to the behaviour of other states.

Naturally, not all problems of international life, and not all uses of ICTs by states require, or are susceptible to, being solved by international law. More granular discussion is therefore needed on particular issues to determine which international solutions are required. Answers to issues of international cybersecurity can be found - and should equally be sought and pursued - in diplomacy, cooperation, technology, trade and other economic affairs, and education. International law, as Kennedy observes, is likely to shape the outcome in international bargaining only where there appears to be a prevalent agreement on the matter among international lawyers.11 Many states regard cybersecurity primarily as a domestic legislative task.12 The US has clarified this relationship between domestic and international law:

“The tasks of Member States are twofold: domestic and international. Securing national information infrastructures is a responsibility Governments must lead on domestically, in coordination with relevant civil society stakeholders. At the same time, domestic efforts should be supported by international collaboration on strategies that address the transnational nature of the various threats to networked information systems”.13

Finally, the fact that international law is debated loudest on matters of international security should not mean that this focus be prominent in European attempts to promote a rules-based international order. Europe’s experience with international law goes well beyond security concerns.

3 What is responsible state behaviour14

The concept of responsible state behaviour is central to contemporary international cybersecurity debates. The term was brought to the issue-set of international cybersecurity in a report of a UN Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013.15 It quickly proliferated through numerous governmental statements. The 2018 Paris Call for Trust and security in cyberspace invites widespread acceptance and implementation of international norms of responsible behaviour as well as

11 Ibid.
12 This was also a long-standing EU view. Sweden, on behalf of the States members of the European Union that are Members of the United Nations, submitted in 2001: it is first and foremost both the right and the responsibility of every country to protect its own information and information-based systems (UN Document A/56/164). For further national views on this see, for instance Guatemala and Syria in A/57/166, El Salvador in A/58/373, Argentina and Costa Rica in A/59/116, Jordan, Qatar and United Arab Emirates in A/61/161, Brunei, Burkina Faso and Lebanon in A/62/98, Niger in A/63/139, Lithuania, Serbia and Ukraine in A/64/129, Mali in A/64/129/Add.1, Ecuador and Portugal in A/66/152/Add. 1, Spain in A/68/156, Iran and Oman in A/68/156/Add. 1, Serbia in 71/172, Poland 3
13 A/66/152.
14 Discussion in this section builds on the opening remarks of Ambassador Marja Lehto.
confidence-building measures in cyberspace. The renewed expert dialogue on international cybersecurity in the UN explicitly focuses on “advancing responsible State behaviour in cyberspace in the context of international security”. In 2019, responsible state behaviour was addressed in the Dinard Declaration on the Cyber Norm Initiative adopted by the G7 Foreign Ministers Meeting and the Declaration of the High Representative on behalf of the EU regarding respect for the rules-based order in cyberspace. The UN High-Level week of 2019 saw a group of states issuing a “Joint Statement on Advancing Responsible State Behavior in Cyberspace” (hereinafter the Joint Statement).

Whether responsible state behaviour is a concept that encourages states to apply a higher standard to their use of ICTs than that shared under international law remains to be seen. Originally, norms, as discussed in the UNGGE, were seen as deriving “from existing international law relevant to the use of ICTs by States”. Since 2015, norms, rules, and principles of responsible state behaviour are considered explicitly voluntary and non-binding. Israel has stressed the importance of this move: “As mentioned in the report, one objective is to identify further voluntary non-binding norms for responsible safe behaviour in order to increase stability and security in the global ICT environment. Future groups of governmental experts should therefore maintain a clear distinction between existing international law, on the one hand, and voluntary non-binding norms on the other, in order to continue to facilitate a broad base for international consensus and in light of rapid technological advances in this field”.

It is essential to follow the international dialogue on responsible state behaviour and determine whether the proposed norms, rules, and principles are indeed intended to promote and enhance international law or whether "responsible state behaviour" is a deflected route around international law.

"We underscore our commitment to uphold the international rules-based order and encourage its adherence, implementation, and further development /.../. We reiterate that human rights apply and must be respected and protected by states online, as well as offline, including when addressing cybersecurity. /.../As responsible states that uphold the international rules-based order, we recognize our role in safeguarding the benefits of a free, open, and secure cyberspace for future generations. When necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behavior in cyberspace”.

---

19 The renewed expert dialogue on international security was addressed in the Dinard Declaration on the Cyber Norm Initiative adopted by the G7 Foreign Ministers Meeting and the Declaration of the High Representative on behalf of the EU regarding respect for the rules-based order in cyberspace.
21 A/68/98, para 16.
22 A/70/174, para 9.
24 US Department of State (2019).
What exactly responsible state behaviour is, and its relationship with international law, remains to be seen. Here, Europe can set a strong example. Voluntary and non-binding norms, rules, and principles of responsible state behaviour can, and will, elicit a higher standard of conduct than the international status quo. Indeed, European states hold themselves to those, and possibly higher, standards of behaviour. As such, responsible state behaviour can be construed as the best practices of international law. However, the concept of responsible state behaviour could also become the worst practices of international law - the minimum of what, under the law, can bear as acceptable practices. In the latter case, emphasis on voluntarism can be construed as an attempt to reject the applicability of some of the international rules and standards in the context of particular national interests related to information and communication technologies.

4 How does international law apply?26

The optionality27 of international law puts a special burden on states seeking to promote rules-based order. States’ prerogative of creating, interpreting, and enforcing international law places upon them a responsibility to take stands on international law. Applying international law in cyberspace is a process that depends on informed, and perhaps consolidated, choices about whether, when, and how to invoke international law in conjunction to states’ uses of ICTs. Tsagourias explains that international law can be invoked through its identification, interpretation, implementation, and enforcement.

Law identification focuses on determining which norms of international law could or should be consulted or actioned in a given situation. Unlike in domestic law, the vast majority of the rules of international law are vague, offering the subjects of international law a degree of flexibility and adaptability in the interpretation and application of these norms. Cyberspace poses particular challenges to law identification because operations or conduct can be covert, indistinguishable, or anonymous. This has given rise to questions as to whether international law applies at all, and if it does, which regulatory framework and which specific rules would apply to a specific conduct. For example, without attribution, international law cannot be applied whereas anonymity is the vanishing point of the law. Furthermore, because of the complex nature of operations (Is the introduction of malware an act of sabotage? Espionage? Use of force?) it is difficult to determine which international law regime applies and this is critical because different regimes may produce different consequences.

Law interpretation focuses on the content and limits of identified rules and standards. It is about establishing normative boundaries, giving meaning to words and applying the law to a set of facts. Rule interpretation can make rules under-inclusive or over-inclusive. Interpretative challenges are not new to international law and they are exacerbated by the fact that international law is either auto-interpreted or interpreted in diverse fora. For example, if the interpretation of cyber force is debated, the application of the law to specific incidents is contested. Interpretative challenges are also exacerbated by the indeterminacy of facts due to the indistinguishable nature of cyber operations. The central question on the delineation of the norms of international law as they apply to cyber operations is where the line should be drawn between

26 This section builds on the remarks and input papers and remarks of Professor Nicholas Tsagourias, François Delerue and Russell Buchan.
what must be agreed between states and what should be left for the unilateral interpretation of each state. What should be settled and enshrined within the rules and what should be left for interpretation?

The principle of state sovereignty offers an example. According to Delerue, this principle has multiple dimensions where it is necessary to determine whether a consensus is needed or if it already exists, or whether these dimensions can be left unsettled and defined unilaterally by each state. Delerue holds that the nature of "sovereignty" is not settled: While some states and scholars consider it a principle, others consider it a rule of international law. For instance, France recently defined sovereignty as a rule of international law, while the United Kingdom considers it only a principle. There is no consensus on the extent of this principle, i.e. what constitutes state sovereignty over cyberspace. Furthermore, a variety of approaches exist when it comes to characterising a violation of territorial sovereignty through cyber operations. There are three main views on this question according to which:

- any cyber operations penetrating a foreign system could constitute a violation of sovereignty. In one reading, this is the French approach. It could be also construed as the approach by states with absolutist readings of sovereignty;

- a cyber operation penetrating a foreign system constitutes a violation of sovereignty only if it meets a threshold of harm. This is, for instance, the approach adopted in the Tallinn Manual 2.0 and by the United States;

- territorial sovereignty cannot be breached by a cyber operation, unless it constitutes a violation of the principle of non-intervention. This is, for instance, the British approach.

This example, no doubt, demonstrates the diversity of acceptation of states and scholars on a specific norm of international law. As importantly, however, it also poses a question about the ability of international law as a system to regulate malicious cyber operations. Most views we elicit about international law in the context of state uses of ICTs are views about international law in general. Absent cyber-specific rules and standards of international law, our arguments about any article of the UN Charter become our assessment of that provision, not its particular use in cyberspace. As Buchan stresses, it is therefore important to broaden our analysis and to explore the impact of the "sovereignty as a principle, not as a rule" thesis on the ability of international law as a system to regulate malicious cyber operations.

Are we setting too hard, or too many, expectations for the principle of non-intervention? Is our denial of any regulatory gaps placing an excessively large burden on single concepts, rules, or principles, thus

29 Ibid. However, some reviewers read the French position more similar to the UK’s position, concluding that at p. 6, the French Ministry of defence only says that any cyber operation may constitute a violation of sovereignty. At p. 7 it specifies that this is the case, if the operation qualifies as a cyberattack (see definitions of ‘cyber operation’, including espionage, and ‘cyberattack’ at p. 18 of the report) or produces effects. Page 6 of the French report: "Toute pénétration d’origine étatique non autorisée sur les systèmes français ou toute production d’effets sur le territoire français par un vecteur numérique peut constituer, a minima, une violation de souveraineté." Page 7:"Toute cyberattaque à l’encontre des systèmes numériques français ou toute production d’effets sur le territoire français via des moyens numériques par une organe étatique, une personne ou une entité exerçant des prerogatives de puissances publique ou par une personne ou des personnes agissant sur les instructions ou les directives ou sous le contrôle d’un Etat est constitutive d’une violation de souveraineté”.
32 See Russel Buchan’s input paper.
rendering them useless? Buchan’s call to resist claims that sovereignty is not a rule of international law is not about “cyber law”. It is a matter of international law and the very international legal order. Who is to stand up for international law in the cybersecurity debate? Or as Hollis frames it: Who is to speak for the trees and confront environmental destruction? There is a quest for states and scholars to help us clarify the content and scope of individual rules and our thinking about how these principles and rules fit together and how they form an international legal system that is able to meet the core needs of the international society in a digital world.

States apply international law every day by implementing it, i.e. acting in ways they deem consistent with their rights and obligations and abstaining from acts they consider inconsistent with international law. In particular, the laws of friendly relations, peaceful settlement of disputes, sovereignty, jurisdiction, or human rights apply seamlessly. All these areas of law merit further research and exposure to explain how states activate and use international law in the majority of their international dealings. As states activate international law through their actions, its applicability is hardly about views or behaviour of any one state - international law becomes evident and observable through the behaviour of the international community. In this context, it is essential to acknowledge and contextualise individual national views on international law, especially in the context of competition, contestation, and acute differences. The recently published national views on the applicability of international law to cyber operations differ to a significant extent, and not just between the United States and Russia but also among like-minded states and even North Atlantic Treaty Organization allies. This invites attention to the true extent of the “like-minded differences”. In this context, it was suggested that closer study is required to determine whether some states have expressed different views on international law in the context of cybersecurity than they have on the same rules and principles of international law in a different context.

Problems with law identification, interpretation, application, and enforcement in the context of cyberattacks and other issues of international cybersecurity have led some authors to argue that international law is in crisis.

It is not hard to see why international law rarely becomes, primarily or only, about enforcement - the interpretations and implementation often order international affairs enough to avoid legal processes like those of the UN Security Council or the International Court of Justice. Uniform practices of enforcement can be complicated by interpretative challenges, disparities in capabilities, or political calculation.

Problems with law identification, interpretation, application, and enforcement in the context of cyberattacks and other issues of international cybersecurity have led some authors to argue that international law is in crisis. These issues, however, are not particular to cybersecurity and to various degrees affect international law in general. Also, despite potential applicability, there is no guarantee of the effectiveness of the identified rules, principles, and frameworks. To wit, the applicability of international law should not be measured or addressed solely by state actions and statements. Views on applicability can be enhanced, supported, and encouraged through activities that promote the international rule of law, an understanding and awareness of it, as

---

33 Duncan Hollis introduced the participants of the International Law workshop to Dr. Seuss’s Lorax (https://www.imdb.com/title/tt1482459/) and suggested that the current stage of the international law and cybersecurity debate could be inspired by the Lorax figure. Further to what international law is and how it can be applied, see also Duncan Hollis and Barrie Sander (2018) Four Challenges for International Law and Cyberspace: Sartre, Baby Carriages, Horses, and Simon & Garfunkel, available at https://www.cfr.org/blog/four-challenges-international-law-and-cyberspace-sartre-baby-carriages-horses-and-simon-0.

34 For instance, Australia, the UK, Estonia, Russia, the US, the Netherlands, Germany, France.


36 See Andrey V. Krutskikh, and Anatoly A. Streltsov (2020) chapter in the Routledge Handbook of International Cybersecurity (footnote 40).
well as considerations behind particular interpretations or positions. A more nuanced and transparent discussion among states on how they understand and use international law could help avoid unwanted developments in state uses of ICTs.

5 International cybersecurity issues

5.1 The state of cyberconflict

Conflict is a social condition arising between two or more parties who have incompatible and unfulfillable requests vis-à-vis each other. In international affairs, two distinct readings with different normative assumptions can be applied to this concept. According to a political reading, conflicts are predominately associated with contestation and violence between states or other politically organised groups. As such, conflict becomes associated with thresholds, such as the use of force or armed attack. A spatial view regards conflict as a stage between peace and war, a grey zone of activities that are not clearly regulated but that are definitely unfriendly. This space cannot be substantiated with clear reference to what has been agreed between states. It derives its weight from state practice and behaviour.

Claims and studies of cyberconflict are diverse. Ranging from cyber doom scenarios to reports of cyber warfare to questioning the war-like nature of uses of ICTs, the portrayed role of ICTs in conflict as well as their susceptibility to inciting or moderating conflict remains inconclusive at best. Noting the Russian Federation’s original (1998) concern that ICTs would come to be used in ways that would violate international law, turned into weapons of mass destruction, and represent a threat to international peace and security, participants discussed publicly known state-affiliated cyber incidents to better understand the current politico-military uses of these technologies. As of June 2019, the Council of Foreign Relations’ (CFR) Cyber Operations Tracker reports more than 300 publicly known cyber operations.

According to CFR, states use ICTs to conduct cyber espionage (over 80 percent of known cyber operations), defacement, denial-of-service, data destruction, doxing, and sabotage. The CFR analysis is mainly limited to operations conducted by or against China, Iran, North Korea, Russia, the United Kingdom, and the United States. Further studies of the issue indicate cyber power projection also in the context of other established rivalries, such as between India and Pakistan. Nevertheless, it becomes evident from this limited analysis that technically capable governments are engaging in widespread cyber espionage. Some governments have established presence in other governments’ and international organisations’ networks. This presence opens avenues for actual effect-creating operations in or through these networks. There are evident tests of military cyber capabilities on established rivals’ networks. Low-effect cyber operations - e.g. taking critical infrastructure offline, disrupting public communications and online services, destroying data, and sabotaging ICT infrastructure) especially between established rivals - are becoming common.

It follows from the CFR data that most effect-creating state-on-state cyber operations fall within the law of non-intervention, peaceful settlement, and sovereignty. So far, state-on-state cyber operations have been addressed by the international law community predominantly from the perspective of jus ad bellum and from the perspective of operational lawyers.

---

37 The discussion in this section builds on the analysis and input of Mika Kerttunen, Eneken Tikk and Kristine Hovhannisyan.
5.2 ICTs as a threat to international peace and security

There is no universal understanding as to whether and how the development and usage of cyber systems and services may threaten international peace and security. Some participants were concerned that ICT means and technologies may potentially be used for purposes inconsistent with the objectives of maintaining international stability and security, and some saw the proliferation of cyber military capabilities as being potentially threatening. Some considered the lack of explicit global regulations dangerous, while others had hopes for voluntary norms to support international peace and security.

It was further noticed that three consecutive groups of governmental experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security have not clearly articulated which uses of ICTs constitute a threat to international peace and security, or how. The 2010, 2013, and 2015 reports provide illustrations of potential threats. Table 1 summarises the discussions of cyber threats in the 2nd, 3rd, and 4th UNGGEs.

What is or is not considered conflictual between any two or more states, remains subject to sovereign decisionmaking and does not entirely depend on the thresholds of international law. Nevertheless, it is easy to observe that the problematic thresholds in international law, in the context of international cybersecurity, are not primarily those of the use of force or armed attack. Current cyber operations predominantly invoke the legal concepts of sovereignty, prohibited intervention, the right of self-determination, the obligation of peaceful settlement of international disputes, the principles of good faith, and friendly relations.
Table 1. State use of ICTs and threats to international peace and security. Author’s compilation from the UNGGE 2010, 2013, and 2015 reports.

<table>
<thead>
<tr>
<th>2010</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>The absence of common understandings on acceptable state behaviour with regard to the use of ICTs increases the risk to international peace and security.</td>
<td>There are disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by state and non-state actors.</td>
<td></td>
</tr>
<tr>
<td>Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future.</td>
<td>Terrorist groups use ICTs to communicate, collect information, recruit, organise, plan and coordinate attacks, promote their ideas and actions, and solicit funding. If such groups acquire attack tools, they could carry out disruptive ICT activities.</td>
<td>The use of ICTs for terrorist purposes, beyond recruitment, financing, training, and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.</td>
</tr>
<tr>
<td>There is increased reporting that states are developing ICTs as instruments of warfare and intelligence and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable state behaviour may create the risk of instability and misperception.</td>
<td>A number of states are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between states is becoming more likely. States are rightfully concerned about the danger of destabilising misperceptions, the potential for conflict, and the possibility of harm to their citizens, property, and economies.</td>
<td></td>
</tr>
<tr>
<td>The growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services.</td>
<td>The expanding use of ICTs in critical infrastructures and industrial control systems creates new possibilities for disruption.</td>
<td>The most harmful attacks using ICTs include those targeted against a state’s critical infrastructure and associated information systems. The risk of harmful ICT attacks against critical infrastructure is both real and serious.</td>
</tr>
<tr>
<td>The rapid increase in the use of mobile communications devices, web services, social networks, and cloud computing services increases challenges to security.</td>
<td>States are concerned that embedding harmful hidden functions in ICTs could be used to</td>
<td></td>
</tr>
<tr>
<td>The inclusion of malicious hidden functions in ICTs can undermine confidence in</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
products and services, erode trust in commerce, and affect national security.

The varying degrees of ICT capacity and security among different states increase the vulnerability of the global network. Differences in national laws and practices may create challenges to achieving a secure and resilient digital environment.

5.3 Permissibility of cyber operations

There has been little international conversation on the permissibility of cyber operations in general or on the particular means and methods of conducting such operations. An ICRC report on the potential human cost of cyber operations points out:

"In the view of the ICRC, many of the operations described in the report[41] would be contrary to IHL if carried out during armed conflict. However, there is insufficient consensus today as to the interpretation of IHL in cyber space to provide clear legal protection for the civilian population". [42]

States have expressed their sentiments about the cyber operation against the Organisation for the Prohibition of Chemical Weapons (OPCW). During the 2018 UN First Committee deliberations, Latvia made the following statement:

"We are dismayed by the attempted cyberattack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in April this year. Attempts to undermine the global norm against the use of chemical weapons and to interfere with the work of the OPCW and its investigative mechanisms must be strongly opposed and deterred. We support the intention of the OPCW to strengthen its capabilities in that regard. Latvia also welcomes the steps taken by the host country of the OPCW, the Netherlands, to avert those actions". [43]

Germany and France also condemned the malign cyber operation targeting the OPCW, while commending its successful disruption by the Dutch authorities. [44] Sweden delivered a statement on behalf of the Nordic countries:

---

[41] Incidents discussed included Stuxnet, Flame, BlackEnergy, WannaCry, NotPetya and Triton.
In a separate statement, the EU deplored the “hostile cyber operation” against the OPCW as undermining international law and international institutions.46

More broadly, UNASUR states have shared their “growing concern about the vulnerability of their critical infrastructure and the possible escalation of conflicts driven by cyberattacks”.47 As discussed further in this report, most of states’ public reactions to cyber incidents have avoided categorising respective incidents under international law. For instance, joint statements about NotPetya and WannaCry incidents do not qualify these cyberattacks as violations of international law.48

6 The current discourse

Participants opined that despite frequent suggestions to the contrary, it was not entirely clear that all states indeed agree that the entirety of international law applies to cyber affairs. In this regard, academia and select liberal democracies may have gotten ahead of themselves with respect to other states’ views and conclusions. Despite an exchange of national views on the subject, it seems that many states prefer a wait-and-see approach to identifying answers to mixed questions of fact and law in cyberspace.

A detailed mapping of the many regional and international processes addressing responsible state behaviour in cyberspace is beyond the focus and scope of this report.48 Suffice to say, although several international and regional processes are dealing with the question of responsible state behaviour in the use of ICTs, very few of them explicitly address the applicability of international law to issues of international cybersecurity. This section addresses the trend of national statements about international law, introduces selected national submissions to the UN First Committee, highlights the policies of consequences and restrictive measures, and contours the scholarly debate on the issue.

6.1 National statements about international law and cyber governance

A noteworthy development context is the recent proliferation of national views on international law and cybersecurity. Table 2 lists national statements and remarks on international law, cybersecurity, and cyber operations. Further claims and arguments have been put forward to promote particular national preferences of world order and governance models. Table 3 lists national strategies focusing on international cyber governance and engagement. In general, many national cyber and information

47 A/C.1/70/PV.21, page 11.
49 For an excellent helicopter view, see the contribution of Barrie Sander’s input paper.
security strategies and doctrines contain dedicated sections for international cybersecurity issues but without wider elaborations of international law as such.50

Table 2. National statements on international law, cybersecurity, and cyber operations. Compilation by author.

<table>
<thead>
<tr>
<th>Country</th>
<th>Year</th>
<th>Statement Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>2011</td>
<td>Militärische, völkerrechtliche und rüstungskontrollpolitische Aspekte der Cyber-Sicherheit (in German)</td>
</tr>
<tr>
<td>The Russian Federation</td>
<td>2011</td>
<td>Concept of a Convention on International Information Security</td>
</tr>
<tr>
<td>United States of America</td>
<td>2012</td>
<td>International Law in Cyberspace, remarks by Harold Hongju Koh, Legal Advisor U.S. Department of State at USCYBERCOM Inter-Agency Legal Conference</td>
</tr>
<tr>
<td>Germany</td>
<td>2015</td>
<td>Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare) (in German)</td>
</tr>
<tr>
<td>United States of America</td>
<td>2016</td>
<td>International Law and Stability in Cyberspace, remarks by Brian Egan, Legal Advisor U.S. Department of State at Berkeley Law School</td>
</tr>
<tr>
<td>Australia</td>
<td>2017</td>
<td>Australia’s position on how international law applies to state conduct in cyberspace</td>
</tr>
<tr>
<td>The United Kingdom</td>
<td>2018</td>
<td>Cyber and International Law in the 21st Century, speech by Attorney General Jeremy Wright QC</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>2019</td>
<td>International law in cyberspace: Appendix to the Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace</td>
</tr>
<tr>
<td>Estonia</td>
<td>2019</td>
<td>Estonian official positions on international law in cyberspace, as introduced by the President of Estonia</td>
</tr>
<tr>
<td>France</td>
<td>2019</td>
<td>International Law Applied to Operations in Cyberspace</td>
</tr>
<tr>
<td>Australia</td>
<td>2019</td>
<td>Australia’s Position on the Application of International Law to State Conduct in Cyberspace</td>
</tr>
</tbody>
</table>

Table 3. International cyber strategies. Compilation by author.

<table>
<thead>
<tr>
<th>Country</th>
<th>Year</th>
<th>Strategy Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States of America</td>
<td>2011</td>
<td>International Strategy for Cyberspace</td>
</tr>
<tr>
<td>The Russian Federation</td>
<td>2013</td>
<td>Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020</td>
</tr>
<tr>
<td>Norway</td>
<td>2017</td>
<td>Internasjonal cyberstrategi for Norge (in Norwegian), International Cyber Strategy for Norway</td>
</tr>
<tr>
<td>Australia</td>
<td>2017</td>
<td>Australia’s International Cyber Engagement Strategy</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>2015</td>
<td>Internationale Cyberstrategie ‘Digitaal bruggen slaan’ (in Dutch), International Cyber Strategy</td>
</tr>
<tr>
<td>China</td>
<td>2017</td>
<td>International Strategy of Cooperation on Cyberspace</td>
</tr>
</tbody>
</table>

6.2 Submissions to the First Committee\textsuperscript{51}

Over the past 20 years, states have been invited to share their views on international information security with the UN Secretary-General. In these materials, one can detect recurring themes, agreement as well as differences about possible legal issues and remedies.

States seem to generally agree on the applicability of the UN Charter including the principles of the sovereign equality of states, non-interference in internal affairs, the prohibition of the use of force, as well as the obligation to settle disputes through peaceful means. However, despite the 2013 conclusion that international law applies to state uses of ICTs, the 2015 UNGGE felt compelled to underscore that the UN Charter applies “in its entirety” (para 28 c). State practice, however, has demonstrated that the group’s reference to “the inherent right of States to take measures consistent with international law and as recognised in the Charter” does not necessarily constitute a solid consensus.

References to the UN Charter have been made in conjunction with operational interests. The Netherlands has stated that “if cyber capabilities are used by States, they should be used in accordance with international law, including the UN Charter”.\textsuperscript{52} “Responsible use” of cyber capabilities has also entered the US' rhetoric: "As cyber capabilities become cheaper and easier to acquire, more States are establishing offensive cyber programs. States must use these capabilities responsibly /.../.\textsuperscript{53} In contrast, China applies an absolutist reading to the UN Charter, emphasising the prohibition of the use of force and refusing to address the applicability of Article 51 of the UN Charter as well as IHL to state uses of ICTs. Further individual submissions prioritise different aspects of the UN Charter. A number of states place a particular emphasis on the principle of non-interference and related elements, such as sovereignty. Cuba has stressed the importance of guaranteeing that the use of ICTs “should be fully consistent with the purposes and principles of the Charter of the United Nations, international law, in particular sovereignty, non-interference in internal affairs, and internationally recognised standards of coexistence between States”.\textsuperscript{54} Similarly, Iran has called states to “observe the purposes and principles of the United Nations and their obligations under its Charter, in particular Article 2, paragraph 3, to settle international disputes by peaceful means, the prohibition in Article 2, paragraph 4, on the threat of use of force in any manner inconsistent with the purposes of the United Nations, as well as the prohibition set out in Article 2, paragraph 7, on intervention and interference in the internal affairs of States”.\textsuperscript{55} On the question of prohibition of the use of force as well as the right to self-defence, some states have pointed out the lack of clear understanding of how relevant legal standards would translate to the cyber domain. A recent Chinese input emphasises that “the applicability of the law of armed conflicts and jus ad bellum needs to be handled with prudence. The lawfulness of cyber war should not be recognised under any circumstance. States should not turn cyberspace into a new battlefield”.\textsuperscript{56}

The Chinese stand on jus ad bellum above could explain why Beijing has been reluctant to discuss the applicability of IHL to state uses of ICTs. In contrast, international law on the use of force and international humanitarian law are frequently referred to by the United Kingdom and the United States. The UK regards the existing principles of international law, both on the use of force and the law of

\textsuperscript{51} This section incorporates, and builds on, Elaine Korzak’s analysis of national views on international law as expressed in the UN First Committee process.

\textsuperscript{52} UN General Assembly 2015a, p 7; Dutch Ministry of Foreign Affairs 2015, p 4.


\textsuperscript{54} UN General Assembly, Report of the Secretary-General A/69/112, p. 9.

\textsuperscript{55} UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 12.

\textsuperscript{56} China (2019) statement at the OEWG.
armed conflict, as providing "an appropriate framework". The United States argues that existing principles of international law serve as the appropriate framework and that "here are two distinct but related bodies of law to consider in this regard: jus ad bellum and jus in bello". Canada confirms that "the Canadian Forces' active cyber capability will be subject to the same rigour as other military tools, including applicable international law and rules of engagement".

With regard to the jus ad bellum, the US submissions highlight three provisions of the UN Charter, namely the prohibition on the use of force (Article 2(4)), individual and collective self-defence (Article 51), and collective measures authorised by the UN Security Council (Articles 39, 41, and 42). In discussing the right to self-defence, the US concludes that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack". Similarly, the US asserts that the following principles of international humanitarian law would play an "important role in judging the legality of cyberattacks during an armed conflict", namely the principles of distinction and proportionality as well as the prohibition on indiscriminate attacks. More importantly, "targeting analysis would have to be conducted for information technology attacks just as it traditionally has been conducted for attacks using kinetic (conventional and strategic) weapons".

The application of international human rights law is mentioned by a vast majority of states in their national submissions. Frequent reference is made to the right to privacy and freedom of expression. Western states place an emphasis on the connection between the application of human rights law and an open and free Internet or cyberspace. Canada emphasises its "strategic interest in preserving an open cyberspace". The Netherlands affirms its support for the "protection of an open, free Internet respecting human rights". With this emphasis on a free and open Internet, many Western states concomitantly express their concern that cybersecurity efforts may be used as a pretext to restrict the free flow of information. The United Kingdom expresses this clearly, stating that it "does not recognise the validity of the term 'information security' ... since it could be employed in attempts to legitimise controls on freedom of expression beyond those agreed in the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights".

In contrast to this understanding, non-Western countries emphasise that international human rights and freedoms apply in their national context. International human rights and freedoms are applicable but are to be implemented within the context of every individual state. Iran holds that "[t]he right to freedom of expression should be fully respected". Yet, "[a]t the same time, this right, in no case, should be exercised contrary to the purposes and principles of the United Nations, national laws and the principles of protection of national security, public order, public health or morals and decency". Qatar asserts that the application of universal human rights needs to be balanced with the need to respect national differences. Accordingly, the "free flow of information must be guaranteed without prejudice

57 UN General Assembly, Report of the Secretary-General A/65/154, p. 15.
58 UN General Assembly, Report of the Secretary-General A/66/152, p. 18.
59 UN Developments in the Field of Information and Telecommunications in the Context of International Security (A-72-315)
60 UN General Assembly, Report of the Secretary-General A/66/152, p. 18.
61 UN General Assembly, Report of the Secretary-General A/66/152, p. 18.
62 UN General Assembly, Report of the Secretary-General A/66/152, p. 17.
63 UN General Assembly, Report of the Secretary-General A/66/152, p. 19.
64 UN General Assembly, Report of the Secretary-General A/68/156, p. 5; UN General Assembly, Report of the Secretary-General A/64/129, p. 10; UN General Assembly, Report of the Secretary-General A/66/152, p. 3.
65 UN General Assembly, Report of the Secretary-General A/66/152, p. 19-20
66 UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 3.
67 UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 15.
68 UN General Assembly, Report of the Secretary-General A/69/112; Full submission of the United Kingdom Foreign and Commonwealth Office 2014, p 1.
to national sovereignty and while maintaining security and respect for cultural, political and moral differences among nations.\textsuperscript{71} Preserving cultural and political differences is equally paramount for the People’s Republic of China, which argues that the “free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected”.\textsuperscript{72} Iran has further argued that, among other things, states should refrain from the use of information and communication technologies for the “transboundary dissemination of information in contravention of international law, including the Constitution and regulations of the International Telecommunication Union, or national legislation of targeted countries”.\textsuperscript{73} Other countries, such as Syria, even call for an internationally enforced ban on disinformation. Accordingly, “[i]nternational standards and rules on the dissemination of information regarding the history, civilisation and culture of peoples in databases and information networks (Internet) must be established, banning disinformation through the dissemination of erroneous information and calling for the adoption of appropriate measures, including the means to take action against parties who commit violations”.\textsuperscript{74} States have made numerous references to the need to uphold and promote human rights online as well as offline, yet with differing understandings of what relevant rights and freedoms contain and how to best guarantee them. Despite the many references made to the international human rights law, the UNGGE has not treated this question on much detail. The 2015 report states in paragraph 13 (e) that “states, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection, and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression”. This provision, however, is incorporated in the “voluntary and non-binding” norms section of the report.

National submissions also acknowledge that sovereignty applies in cyberspace, entailing both rights and responsibilities for states. Greece notes that sovereignty should be understood as the basic reference for every attempt of globalisation.\textsuperscript{75} According to Sweden, “[i]t is first and foremost both the right and the responsibility of every country to protect its own information and information-based systems”.\textsuperscript{76} Brazil underscores that all countries have equal rights regarding the protection of their homeland against cyberattacks.\textsuperscript{77} In its 2013 report, the Group of Governmental Experts mirrored this sentiment by stating that “[s]tate sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities, and to the jurisdiction over ICT infrastructure within the territory”.\textsuperscript{78}

Some states concerned with the use of proxies underline states’ responsibilities with regard to the actions of non-state actors. According to South Korea, “[s]tates must meet their international obligations regarding internationally wrongful acts attributable to them”.\textsuperscript{79} To that end, “[s]tates must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs”.\textsuperscript{80} Likewise, the United States acknowledges the problem that “[a]cting through proxies significantly increases States’ ability to engage in attacks with

\textsuperscript{71} UN General Assembly, Report of the Secretary-General A/65/154, p. 9.
\textsuperscript{72} UN General Assembly, Report of the Secretary-General A/61/161, p. 4.
\textsuperscript{73} UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 13.
\textsuperscript{74} UN General Assembly, Report of the Secretary-General A/57/166/Add. 1, p. 6.
\textsuperscript{75} UN General Assembly, Report of the Secretary-General A/65/154, p. 6.
\textsuperscript{76} UN General Assembly, Report by the Secretary-General A/68/98, para. 20.
\textsuperscript{77} UN General Assembly, Report of the Secretary-General A/64/129, p. 4.
\textsuperscript{78} UN General Assembly, Report of the Secretary-General A/66/152, p. 20.
\textsuperscript{79} UN General Assembly, Report of the Secretary-General A/70/172, p 12; South Korean Ministry of Foreign Affairs 2015, p 4.
\textsuperscript{80} UN General Assembly, Report of the Secretary-General A/70/172p 12; South Korean Ministry of Foreign Affairs 2015, p 4.
plausible deniability".81 And "[w]hile existing international law has provisions governing the use of mercenaries, the use of proxies in cyberspace raises new and significant issues with wide-ranging implications".82

Another subset of states highlights the responsibility to combat terrorism, asserting that existing legal obligations "apply fully when terrorists or terrorist facilitators use cyberspace to recruit, raise funds, move money, acquire weapons or plan attacks". Thus, "[a]ll States are obliged to share information about, and to take action against, online terrorist financing, recruitment, planning and facilitation activities, while respecting the sovereignty of other States and their own responsibilities to allow the free flow of information".83

As these two concerns indicate, one of the main challenges of applying the law of state responsibility to cyberspace lies in the level of due diligence required by the state for actions of non-state entities. This aspect remains unaddressed by national submissions, although this does not diminish its significance. As the Netherlands eloquently summarises, "[o]f particular importance is the examination of ... the question of how the principle of State sovereignty applies to State activities in cyberspace, consistent with States' international obligations and the law of State responsibility. It also includes the question of the application of the principle of due diligence, i.e. not to knowingly allow a State's territory to be used for acts contrary to the rights of other States".84

The application of state sovereignty is seen as being rather uncontroversial, so the main contrast emerging among states' submissions concerns its reach. In other words, what is the regulatory reach of national jurisdictions in cyberspace and what are the limits to the exercise of sovereign rights? The emphasis of sovereign rights in the application of international human rights law is an example of this controversy that has already been discussed. In addition, some states stress the importance of sovereignty in limiting undue interference. The government of Venezuela, for example, holds "that any violation of information security is contrary to the legitimate right of States to full exercise of their sovereignty. Hence the use of information technologies and media for the purpose of political and economic destabilisation is contrary to the fundamental rules of democracy".85 Lastly, states recognise that sovereignty does not only come with rights but also responsibilities, attaching legal responsibility to their actions in cyberspace and, under certain circumstances, to the actions of non-state actors.

The Russian Federation's views on international law have largely remained the same since the inception of the UN First Committee process. In 1999, Russia submitted a list of issues that, in their reading, require an international legal basis. In the Russian conception, international law is currently unequipped, for instance, to guide the proper classification, and therefore the prevention, of information wars, the identification of the means and methods of information warfare, the prevention of the proliferation of information weapons, and the use if ICTs against critical infrastructure.86 Moscow has also long held that international regulation of the use of information technologies and means for terrorist or other criminal purposes would require an international agreement.87 In its 2000 submission, Russia proposed a set of principles of international information security.88

That Russia's position on these issues has not significantly changed can be read from more recent comments on the subject. Its concept for a Convention on International Information Security can be

82 UN General Assembly, Report of the Secretary-General A/66/152, p. 19.
83 UN General Assembly, Report of the Secretary-General A/66/152, p. 20.
84 UN General Assembly, Report of the Secretary-General A/70/172, p 7; Dutch Ministry of Foreign Affairs 2015, p 4.
86 UN General Assembly, Report of the Secretary-General A/54/213, pp. 8-11.
87 UN General Assembly, Report of the Secretary-General A/54/213, pp. 9.
88 UN General Assembly, Report of the Secretary-General A/55/140, pp. 3-7.
found on the website of the Ministry of Foreign Affairs of the Russian Federation.\textsuperscript{89} This text repeats several provisions of the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization.\textsuperscript{90} International law will need to be further developed where states cannot demonstrate its applicability or where gaps are identified in the current legal frameworks. In a 2014 article, ambassador Krutskikh and professor Streltsov leave the reader with 27 questions about how international law can be applied to cyberspace, expressing hope that these questions will help structure the international debate.\textsuperscript{91} And more recently, they argue that international law is in crisis.\textsuperscript{92}

6.3 Further views

It has long been perceived that a limited number of countries, led by Russia and China, prefer a treaty approach to international cybersecurity. However, national views recorded in the UN General Assembly and First Committee show some degree of support to this prospect. Those who point out the limitations of the current discourse include regional leaders and EU Member States.

According to Brazil, "the recognition that international law and the principles of the Charter of the United Nations apply to State behaviour in their uses of ICTs leads the way to a peaceful and stable digital environment. In addition, the international community must examine the need to develop a specific legal framework to deal with the challenges we face in this realm".\textsuperscript{93} Brazil holds the view that any reassurance that ICTs will not be used as instruments of aggression should include a no-first-use norm with regard to offensive operations that use ICTs.

Concluding that the economy and day-to-day life would be inconceivable without information and digital technology, Qatar stresses the need to regulate how cybersecurity issues are dealt with. Doha has proposed convening an international conference to examine means of regulation through international law in that area and has expressed readiness to host such a conference.\textsuperscript{94} Pakistan considers it "essential to develop universally agreed legal frameworks in the area of cybersecurity, lethal autonomous weapons systems, artificial intelligence and the weaponization of outer space".\textsuperscript{95}

Slovakia has expressed concern about growing manipulation through social media that is undermining democracy and indoctrinating populations worldwide. Slovakia calls upon states to set new standards and, where needed, regulations - "because today we do not lead, we only follow. And the price of inaction may soon be very high".\textsuperscript{96} Serbia points out that unregulated cyberspace diverts resources that could otherwise be invested in other critical areas.\textsuperscript{97}

The Non-Aligned Movement (NAM), established in the midst of the collapse of the colonial system and currently composed of 120 states, has also made clear statements to this end: As information and communications technologies have the potential to endanger international peace and security, countering such emerging security challenges and reducing their risk is essential. The development of


\textsuperscript{90} Concluded on 15 June 2009.

\textsuperscript{91} Andrey V. Krutskikh and Anatoly A. Streltsov (2014) Международное право и проблема обеспечения международной информационной безопасности. In: Международная жизнь № 11-2014.

\textsuperscript{92} Andrey V. Krutskikh and Anatoly A. Streltsov, A.A. (2020).

\textsuperscript{93} A/C.1/71/PV.4, page 8.


\textsuperscript{95} Pakistan, in A/73/PV.14, page 46

\textsuperscript{96} Slovakia, in A/73/PV.7, page 39

\textsuperscript{97} Guyana, in A/73/PV.12, page 5
a legal framework to address these issues should be pursued within the United Nations, with the active and equal participation of all states.98

Where it is felt that international law would require clarification or debate, the pros and cons of this process should also be critically assessed. Acting under existing law requires working through extensive (and different) experiences and available normative material. It takes a willingness to be bound by decisions made by earlier and "external" actors. At the same time, this approach promises coherence and continuity of the international legal order. A *lex specialis*, or new law, approach offers freedom to decide on rules and principles of current liking, rejecting automatic application of old law and others' decisions. Such an approach, however, runs the risk of leaving truly problematic and disputed things unregulated. Moreover, especially coinciding with a politically contested issue-set, this approach may not succeed, stalling full focus on existing law.99

### 6.4 Consequences of ‘bad behaviour’ in cyberspace

As another recent development, the US and like-minded states have started to "enforce" voluntary norms, rules, and principles of the 2015 UNGGE report. Such a move could be considered as an attempt to safeguard the consensus legacy of previous UNGGE reports. However, it can also be read as their attempt to enforce their reading of international law.

States have taken steps to ensure the implementation of the "voluntary and non-binding" norms, including by way of retorsion - unfriendly acts against states that do not rise to the standard of *expected* behaviour. The USA has had a system in place since 2015 for imposing sanctions on individuals and entities that are determined to be responsible for, or complicit in, malicious cyber activities that result in specific harm likely to constitute or contribute to a significant threat to the national security, foreign policy, economic health, or financial stability of the country.100 The EU has followed the suit with their own twist. In June 2017, the EU Foreign Affairs Council endorsed the main principles of a framework for a joint EU diplomatic response to malicious cyber activities - the so-called Cyber Diplomacy Toolbox.101 The Council’s conclusions mention a series of possible measures within the framework of the Common Foreign and Security Policy that EU institutions and Member States could undertake, from diplomatic demarches to public statements, as well as the possibility of support to other Member States and restrictive measures. In May 2019, the Council established a further framework102 which allows the EU to impose targeted restrictive - travel and economic resources affecting - measures to deter and respond to cyber attacks which constitute an external threat to the EU or its Member States. The

---

sanctions regime, summarised in Table 4 by the criteria used to assess potential targets of sanctions, also covers cyberattacks against third states or international organisations.

Table 4. EU restrictive measures as per Council Decision 7299/19 on 14 May 2019.

<table>
<thead>
<tr>
<th>External</th>
<th>Cyberattack</th>
<th>Significant</th>
<th>Threatening</th>
</tr>
</thead>
<tbody>
<tr>
<td>originate, or are carried out, from outside the EU</td>
<td>access to information systems</td>
<td>the scope, scale, impact, or severity of disruption</td>
<td>critical infrastructure</td>
</tr>
<tr>
<td>use infrastructure outside the EU</td>
<td>information system interference</td>
<td>number of entities affected</td>
<td>maintenance of essential social and/or economic activities</td>
</tr>
<tr>
<td>are carried out by an entity established outside the EU</td>
<td>data interference</td>
<td>number of Member States concerned</td>
<td>critical state functions</td>
</tr>
<tr>
<td>are carried out with the support, at the direction, or under the control of an entity operating outside the EU</td>
<td>data interception</td>
<td>amount of economic loss; economic benefit gained</td>
<td>classified information</td>
</tr>
</tbody>
</table>

Sanctions will be implemented against persons and organisations listed in the annex to the legislation. Listings will require unanimous vote by EU Member States. No listings have so far taken place.  

Such “enforcement” of voluntary norms and principles is a noteworthy development for several reasons. Firstly, retorsion is a way, albeit a silent one, of applying international law to activities in cyberspace. Through their responses, states are likely to clarify which responses to “bad behaviour” are permissible under international law. Responses may also make states’ views on what is and what is not considered a violation of international law more visible.

“When necessary, we will work together on a voluntary basis to hold States accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law”.

103 Cyberattacks are defined in the legislation as “actions involving […] access to information systems; information system interference; data interference; or data interception where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned”.
105 Ibid.
Most known cyber incidents have not been framed as violations of states’ international obligations. However, serious doubts remain about both the significance and status of consequences in terms of international law. For instance, in June 2019, the US conducted a cyberattack against Iran in response to Iran’s alleged attacks on oil tankers in the Strait of Hormuz and the downing of a US surveillance drone.\footnote{See Julian E. Barnes (2019), U.S. Cyberattack Hurt Iran’s Ability to Target Oil Tankers, Officials Say, The New York Times, 28 August 2019 \url{https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html}.} The US Administration has reportedly also considered cyberattacks against Iran in response to the drone attacks on Saudi Arabian oil installations. Such practices call for closer legal and political scrutiny of the like-minded views on international law.

Participants noted that in practice, “consequences” can range from diplomatic demarches to public attribution and from restrictive measures to cyber operations. Much of this is certainly useful to ensure accountability for, and to prevent, malicious cyber operations. However, the less orderly the response, the closer we are to “fighting fire with fire”.\footnote{Cf. Melissa Hathaway (2019) Patching our Digital Future Is Unsustainable and Dangerous”, CIGI Papers, No. 201.}

### 6.5 Scholarly debate\footnote{This section builds on the input by Barrie Sander and Professor d’Aspremont.}

A thorough examination of the many valuable scholarly contributions to the discussion of international law and cybersecurity remains beyond the scope of this paper. Sander summarises that within the field of peacetime cyber governance, international lawyers have pursued at least three different modalities of engagement.\footnote{Cf. Barrie Sander (2017) Cyber Insecurity and the Politics of International Law, 6 ESIL REFLECTIONS, 9 June 2017.}

- **Law Articulators:** International lawyers have engaged with issues of peacetime cyber governance by examining the extent to which existing international legal frameworks already apply to cyber activities, often adopting a law-by-analogy interpretive approach whereby “the extent to which cyberspace and the context that generated the existing rule are similar (or dissimilar) serves to delimit the basic boundaries of the existing international law” (D.B. Hollis, “Re-thinking the Boundaries of Law in Cyberspace” in J.D. Ohlin et al. (eds), Cyber War: Law and Ethics for Virtual Conflicts (OUP, 2015) 129, at 144).

- **Law Entrepreneurs:** International lawyers have engaged with issues of peacetime cyber governance by proposing new primary rules identifying affirmative duties related to cyber activities, new secondary rules aimed at overcoming challenges of attributing responsibility for cyber activities, as well as new international bodies - such as attribution organisations - with mandates tailored to the cybersecurity context.

- **Norm Articulators and Norm Entrepreneurs:** International lawyers have also sought to articulate and cultivate peacetime cybersecurity norms, expanding the horizons of their activities in two respects: first, by bringing into analytical focus a broader range of normative bases beyond international law - including political, professional, and cultural commitments; and second, by providing a more flexible avenue for regulating non-state actors, such as individuals and industry actors, free from the strictures of international legal frameworks.

D’Aspremont observes that scholarly debates about cyber activities follow well known patterns of thought found in general international legal scholarship. Although scholarship has moved away from analogical reasoning in recent years, it continues to make highly predictable moves as it perpetuates the routine at work in international legal literature. Thus, cyber international legal scholarship proves orthodox and falls short of any major thought innovation. The five main conservative features of cyber international legal scholarship can be summarised as (1) a self-justificatory spirit of exceptionialism; (2) a continuous quest for complexity; (3) an emphasis on vulnerability and a praise of scholarly chivalry; (4) a specifically tailored disciplinary history; and (5) a controlled self-flagellation (reminiscent of the New...
Haven approach to international law). One can argue that the engagement of international lawyers with cyber activities has been a missed opportunity to renew some of the main categories of international legal thought: international cyber legal scholarship would have been justified in exploding all the common protocols, the dominant spatial organisation of the world, the centrality of territorial thinking, the sources of international law, etc. Instead, international cyber legal scholarship has continued the "recurrent sameness" found in the rest of the international legal literature.

This lack of revolution in legal thinking in this field does not necessarily constitute a problem in and of itself. However, the relative opacity of the international dialogue and the very limited (and targeted) exposure of legal scholars to the intergovernmental debate exacerbate the problem of contained and constrained discussion. Debates of international law and cyberspace are dominated by the experts involved in the Tallinn Manual process. Contesting and alternative views have not gathered critical attention in the international discussions. Participants noted rich scholarly work that opens further perspectives on international law as it may be applied by states. A shared repository would be useful for informing and directing further scholarship and projects. To determine where additional efforts can be most usefully directed, the impact of the Tallinn Manual on legal scholarship and state behaviour merits closer examination.

The current fixation on operations is a preference and prerogative of a relatively small number of states. Their interests should not discourage wider searches for a positive agenda in support of acute international information and cybersecurity issues. International law debates should not be deterred by contingent political stands and framings adopted by individual states. Temptations to be painted as like-mined or "other-minded" may stand in the way of detecting avenues for directing the international dialogue - for instance, could a state’s current behaviour and positions on international law, in particular IHL, signal that with the development of military cyber capabilities, the contested threshold in the context of international peace and security is no longer that of use of force but of prohibited intervention or violation of sovereignty. In particular, the normalcy of international law, its pacifying and de-escalatory face, deserves further attention and internalisation in the cybersecurity discourse.

7 Have we been here before?

7.1 International regimes on the development and use of ICTs

Issues and concepts central to international cybersecurity debate have been subject to decades of contestation. Various related themes have been debated in the United Nations Educational, Scientific and Cultural Organization, the International Telecommunication Union, and the UN Third and Second Committee. International cybersecurity is simply the most current framing of the theme under the First Committee processes and participants and observers of these processes should make no mistake of the actual mandate and focus of the dialogue - that of international peace and security.

\footnote{Any examples here would be a selective fraction of the work done. Participants have started building a repository that will be made publicly available.}
The emergence and disappearance of particular processes from international agendas are noteworthy, as are the persistence and recurrence of the Western quest for the free flow of information and the Russo-Sino focus on state control and sovereignty. Various platforms have been abandoned or marginalised as they have become cumbersome for respective champions.\footnote{For details, see, e.g. Ulla Carlsson (2017) The Rise and Fall of NWICO: From a Vision of International Regulation to a Reality of Multilevel Governance. Nordicom Review, Volume 24, Issue 2, Pages 31–67.} Also, the very framing of “cybersecurity” issues makes it difficult to focus and scope the dialogue and adequately assess its outcomes and impact.

ICT-related threats and challenges to human and international security have been addressed in the UN systematically since the 1960s. The Final Act of the 1968 International Conference on Human Rights, dedicated to the 20\textsuperscript{th} anniversary of the Universal Declaration of Human Rights, included a section on Human Rights and Scientific and Technological Developments (Resolution XI, page 12). Concluding that scientific discoveries and technological advances may endanger the rights and freedoms of individuals, the Conference called for an interdisciplinary study of these problems, including the uses of electronics which may affect a person’s rights.\footnote{Resolution XI of the Final Act of the International Conference on Human Rights, Teheran, 1968 https://legal.un.org/avl/pdf/ha/fatchr/Final_Act_of_TehranConf.pdf} A 1978 UNESCO study concluded that the international information system demonstrated a profound imbalance between developed and developing countries, where developed countries “dominated the information circuit from start to finish”. As a result, 75 countries called for a new world order for information, mainly involving the reorganisation and reconsideration of policies and regulations pertaining to the media, access to information, copyright, and spectrum management.\footnote{International Commission for the Study of Communication Problems, The New World Information Order (Paris: UNESCO, 1978.}

The 2003 Tunis Commitment recognised the need to address threats resulting from the use of ICTs to international stability and security, acknowledging that such uses may adversely affect national security. It concluded that it was necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights.\footnote{WSIS Tunis Commitment, 18 November 2005, para 15.} The UN Resolution on the Global Culture of Cybersecurity posited that as a result of increasing interconnectivity, critical information infrastructures were now exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns.\footnote{A/RES/57/239} It underscored the importance of international cooperation for achieving cybersecurity and the protection of critical information infrastructures through the support of national efforts.\footnote{A/RES/68/167. The resolution was co-sponsored by Argentina, Austria, Bolivia, Chile, Cuba, Democratic People’s Republic of Korea, Ecuador, France, Guatemala, Indonesia, Ireland, Liechtenstein, Luxembourg, Mexico, Nicaragua, Peru, Slovenia, Spain, Switzerland, Timor-Leste and Uruguay.}

In 2012, tensions between states arose over the question of the extent to which governments should be engaged in regulating the Internet. The United States asserted that “governments, consumers, citizens, and society benefit significantly when all market players have the flexibility to innovate and develop new services in competitive markets, in response to consumer demand. Telecommunications markets that are structured in this way attract investment, fuel technological advancement, and are efficient in delivering services to consumers.” For this reason, the United States did not support proposals to amend the International Telecommunication Regulations that would force a change to the operation of competitive markets. In 2013, the question of privacy in the information age was raised in the UN Second Committee by Brazil and Germany.\footnote{116}
In situations where a disruptive technological development has resulted in international peace and security implications, institutionalisation of the issue(s) is a logical course of action. The establishment of the OEWG can be construed as a development towards a more inclusive debate. At the same time, Russia and the US are primarily focused on avoiding developments that might draw them into an incidental conflict. For Russia and China, the OEWG’s primary instrumental value is in gathering a wider audience to confront the US’ and the like-minded’s agenda of a free and open Internet. The longevity of the OEWG is therefore hardly guaranteed and will heavily depend of the outcomes of the UNGGE and the bilateral relations between the USA and Russia.

Participants concluded that lex specialis is an equally logical approach to something as strategically permeating as ICTs and cyber threats. The workshop did not discuss the pros and cons of a cyber treaty but noted that this topic merited a separate discussion.

7.2 Experience from earlier disarmament issues

Participants underlined that the procurement and use of weapons generally precede their specific regulation under international law. Vestner suggested that the emergence of the term international humanitarian law (IHL), the international regulation of Private Military and Security Companies (PMSCs), and the adoption of the Arms Trade Treaty (ATT) may serve as blueprints that offer insights on how the objective of applying international law to cyberspace might be achieved:

a) Change of perception of the international regulation of warfare. The normative evolution of IHL, the development of its protection offered to civilians, and the creation of disarmament treaties complementing the regulation of warfare may offer relevant insights for discussions regarding cyberspace. Yet most interesting is the evolution of the denomination of this body of law. The linguistic move from “law of war” and “law of armed conflict” to “IHL” has arguably changed the general perception and understanding of the law, independent of substantive changes of the law itself. Rather than just a simple normative framework applicable to warfare, “international humanitarian law” suggests that the law mainly serves humanitarian purposes. Accordingly, the balance between humanitarian principles and military necessity would be interpreted so that any war-related action would need to follow humanitarian principles. Notably, representatives of the International Committee of the Red Cross (ICRC) and those arguing for an expansion of human rights to situations of armed conflicts brought about this change by consistently using the term and expanding the scope of its meaning. It can be argued that the change of denomination of the body of law subconsciously influences the way that lawyers, policymakers and operators interpret and apply the law. Regarding the application of international law to cyberspace, this suggests that terms and concepts used may influence thinking and, ultimately, state practice. Even if there is no progress regarding substantive legal issues, strategic and persistent use of terms may influence state behaviour in the long term.

---

117 This section builds largely on the input paper by Tobias Vestner.
118 The ban of blinding laser weapons prior to their use is a notable exception. See: Protocol IV to the Convention on Certain Conventional Weapons, adopted on 13 October 1995.
b) Application of international law to emerging private actors in conflict zones. Since the 1990s and notably the conflicts in Afghanistan and Iraq, states increasingly rely on private entities for providing security services in conflict zones. This had raised concerns that PMSCs would disrespect international norms, as was illustrated by the Blackwater incident in 2007, where 17 civilians were killed in a shootout after one of Blackwater’s convoys was attacked while they were escorting an American diplomatic envoy. Switzerland and the ICRC launched a diplomatic process which led to the 2008 Montreux Document.\textsuperscript{121} Part I of this soft law instrument is a restatement of international (hard) law. While there is no novelty regarding the legal substance, the value of Part I is that states acknowledge the application of international law to the use of PMSCs in armed conflicts as well as derived obligations of states and members of PMSCs. Part II offers good practices to promote compliance with IHL and human rights law during armed conflicts. Designed as politically binding recommendations, Part II was acceptable to states. In addition, the establishment of a self-regulation mechanism by private security providers precluded high regulatory and bureaucratic costs to states. This approach suggests that states could commit to the application of international law to cyberspace through a well confined multilateral process and official document. The pragmatic decision to not challenge states’ use of PMSCs and the limited ambition to only commit states to the application of existing international law may also be lessons applicable to cybersecurity.

c) Codification of national practices through international standards on arms transfers. The ATT was adopted by the United Nations General Assembly in 2013 to establish legally binding restrictions on the control of international arms transfers. Despite non-governmental organisations calling the treaty a historic achievement, the ATT does not establish higher standards than the existing national standards of major exporting states. Indeed, the treaty primarily codifies existing state regulations and practice and establishes international cooperation and assistance mechanisms.\textsuperscript{122} The driving motive for major exporting states was to internationalise their domestic standards and lock in competitors, i.e. to establish a normative level playing field so that they would not be disadvantaged on the international arms market by their restrictive national regulations. Related to cyberspace, this suggests that regulations could first be imposed on the national rather than the international level. States need domestic frameworks to manage their cyber activities and to react to those encountered by other actors. It is unimaginable that states do not invoke or rely on international law for establishing national laws, regulations and policies. Jurisprudence by domestic courts may also do so. Multilateral deadlocks may break up once states have fully developed domestic frameworks and are ready to codify their practices at the international level - eventually at a low cost and with the benefit of gaining legitimacy for their actions.

An approach supported by some academics, states, and shareholders is to design a new regime in line with the particular features of cyberspace (aterritoriality, interconnectedness, etc.) and the presence therein of private actors. Indeed, the prevalence of private actors in cyberspace poses ontological as well as regulatory challenges to traditional concepts and methods of international law. A new regime could address the particularities of cyberspace and incorporate its many stakeholders but it raises questions of legitimacy (the private sector is not a monolithic community so questions as to who should participate arise), location of authority, as well as questions about the nature of the interests pursued and the priorities set (states may pursue different interests than the private sector). A new regime in which states and non-state actors both participate requires a radical revision of how we view international law and what we expect from it.


Useful examples of the private sector championing international agreements do exist in international law, for instance in international environment law. Although cybersecurity is perceived as being much more related to “hard” security than, say, environmental issues, the role of the private sector in progressive development of international law should not be dismissed and the nature of cyber threats might be worth revisiting.

7.3 Inquiries into further fields of (international) law

Throughout the discussions, participants made several references to experiences from other legal areas. Comparative and private international law/economic law approaches could be usefully applied to issues of cybersecurity to elicit true gaps in the current international legal order and determine how to address them. In particular, studies on the comparability of various national approaches could inform the understanding of possible developments, current or future, of international law. Economic law, in turn, can lend expertise for combining national and international solutions to identified and shared issues. Economic law may offer blueprints for mixing and combining national, minilateral, and international solutions to issues of cybersecurity. Issues of jurisdiction deserve further inquiry under private international law. Differences on the issue of data as an object may benefit from research of how various aspects of data have been conceptualised and regulated in the field of intellectual property and personal data protection. It was suggested that in the future, ruminations on international law and international cybersecurity could involve the experience of colleagues who have crafted and delivered similar messages to other focus groups (environmental law, trade law, security policy).

Participants also noted the distinct approach by Russian colleagues, whereby the recommendations of the UNGGE can be implemented through the existing, albeit fragmented, specialised rules of international law. According to that approach, recommendation 13 (g) of the UNGGE (2015) on the protection of critical infrastructure can rely on the Assistance Convention, the Convention on the Transboundary Effects of Industrial Accidents, and the Convention on the Provision of Telecommunication Resources. The above blueprints suggest that the denomination of legal concepts and issues, as well as norm development at the domestic level prior to codification by international law, could be an effective means to advance international law related to cyberspace. Further research could study in detail the need of new international norms and the conditions of their implementation. From a policy perspective, a relevant question is how ambitious regulation attempts should be. It might also be worth reflecting on the opportunity costs of potential normative developments.

Some participants expressed pessimism about blueprints. They recalled that the most effective, momentous, and resilient international legal solutions have been born of calamity. The UN Charter, the Declaration of Human Rights, the Fourth Geneva Convention, and the Genocide Convention all followed cataclysmic failures in peaceful relations. The question thus becomes whether it is realistic to conceive a similarly momentous legal development for cybersecurity in the absence of a preceding cyber catastrophe. The discussion left open the question of the current status of international affairs in this

---

123 Anatoly A. Streltsov and Eneken Tikk (eds) Methodological issues of the application of norms, rules and principles of responsible behaviour of states to promote an open, secure, stable, accessible and peaceful ICT environment (forthcoming 2020).
127 Related questions could be: Shall the application of an entire branch of international law be envisaged or only the application of certain principles? Shall specific and precise norms be crystallised, such as a code on the protection of civilians in cyberspace, or general commitments generated?
context - with the remark that some authors construe the current situation as an international conflict and a failure in peaceful relations.

8 Conclusion

European scholars, like European states, are convinced that international cyber affairs are to be governed by international law. This conviction serves as a common platform on which to invite, introduce, and debate views on how to best apply international law to issues of cybersecurity, since everyone joining this platform is interested in helping to advance international law - and improve international life. That they may have differing views and approaches for how to do this is a sign of the strength, not the weakness, of the European discourse.

The European relationship with international law is long-standing and solid. Our approach to cybersecurity acknowledges it as a combination of domestic, regional, and international efforts in which law - and international law - have a non-negotiable role but are not the only drivers. Europe has demonstrable experience and expertise in self-restraint, escalation control, and conflict prevention. Explicating international law as a framework of peace and stability would need to borrow and combine expertise and experience from various disciplines. It is essential to involve in the dialogue more scholars and experts, including those who have had less exposure to the specialized "cyber" and international law discussion. But it important to mainstream the discussion of these issues and open it up to more than just carefully crafted and promoted views and insights.

As the international cybersecurity discourse indicates, the question of international law and state use of ICTs is far from settled. There are different readings of international law on the table, some of them considerably lighter than what has been a European reading of international law. It is therefore only natural to invite Europe to assume a leading role in moderating international talks on how to apply international law to issues of cybersecurity. Such leadership would require an open, transparent, continuous, and critical dialogue within Europe and in the world. It would necessitate thinking beyond contingent political stands and preparedness to reach unanticipated conclusions. In line with the European values and goals, it would promote and fortify international law. A European approach to applying international law in cyberspace would command a true partnership between governments and academia, determined cooperation between European and non-European scholars, and genuine interest in how to sustain ICTs as a technology of peace and prosperity.

Several questions and thoughts were put on the roster for future discussions. In the context of calls for a specialised legal regime, what is to be regulated and how? In more detail, what do we mean by cybersecurity (if security is a state function, what is the role of private actors)? What is the content and scope of international cybersecurity? What is the object of regulation that arguably already exists or is needed? Is it the Internet, operations, or content? Should all aspects of cyber behaviour and conduct be regulated at once and in one document or separately and gradually? By what type of regulation? Should specific rules with specific methods of enforcement be devised or devise a looser regime of standards and enforcement? Would regulation take the form of a treaty or custom? Should regulation be intergovernmental or multi-stakeholder? Should we allow for self-regulation? Should regulatory action be proactive laying down rules in advance or reactive after a specific event? What can the different stakeholders do to promote international law now or in the future?
About the author

**Dr Eneken Tikk** is affiliate researcher of the Erik Castrén Institute of the University of Helsinki. She is also the Executive Producer of the Cyber Policy Institute. Eneken advised the Estonian expert to the UN Group of Governmental Experts (UN GGE) on developments in the field of information and telecommunications in the context of international security (2012–13, 2014–15 and 2016–17). Eneken has directed the ICT4Peace Foundation’s capacity building program on international cybersecurity, norms and international law (2014-2019). She is an elected member of the board of the Cyber Defence Unit of the Estonian Cyber Defence League. Dr Tikk teaches courses on cyberlaw, state-on-state cyber operations, international law, and GDPR at the Tallinn University of Technology (Estonia) and the University of Jyväskylä (Finland). She is the co-editor of the Routledge Handbook of International Cybersecurity (2020) and the editor-in-chief of the International Journal of Digital Peace and Security (IJDPS).
About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

**RESEARCH IN FOCUS**

is a series of research papers aimed at supporting the EU’s cyber-related policies by providing a timely and policy-relevant analysis.