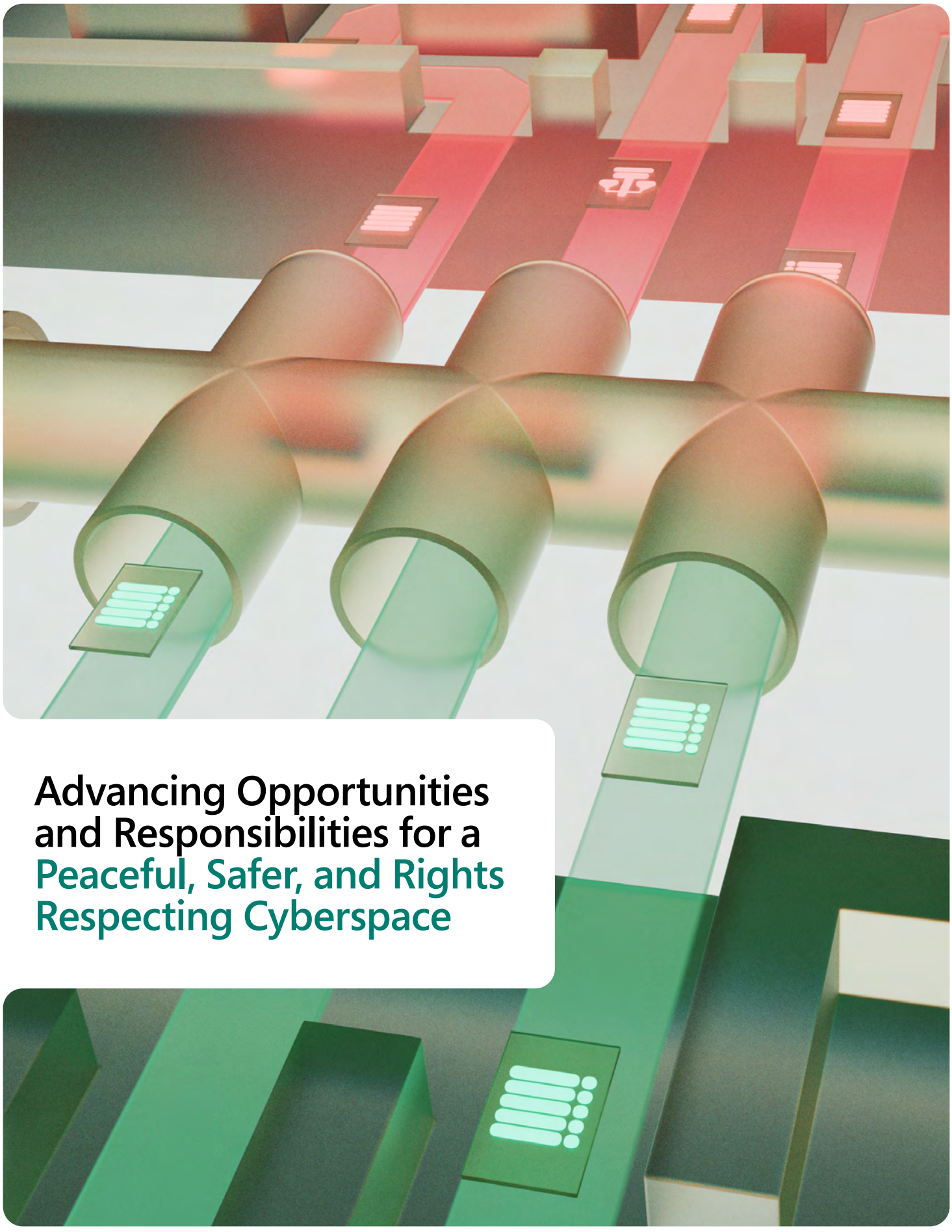


Advancing Opportunities and Responsibilities for a Peaceful, Safer, and Rights Respecting Cyberspace

Microsoft

Temple University
Beasley School of Law

Institute for Law, In
& Technology (iLIT)

RELACIONES EXTERIORES
SECRETARÍA DE RELACIONES EXTERIORES

About this compendium

Throughout the Fall of 2023, the Mexican Ministry of Foreign Affairs, Temple University's Institute for Law, Innovation & Technology (iLIT), and Microsoft brought international lawyers and cross-sector cybersecurity experts together to address the role of international law in making cyberspace peaceful, safer, and rights-respecting. Through three virtual workshops, a diverse array of participants from governments, industry, civil society, academia, and other relevant stakeholders explored how to (i) identify successes and challenges in applying international law to cyberspace; (ii) improve state accountability for online behavior; and (iii) bridge digital gaps and promote access to cyberspace. The presentations and discussions for each workshop generated a robust series of recommendations, lessons learned, and good practices.

Based on what we heard and learned in these discussions, we have developed this *Multistakeholder Compendium on Advancing Opportunities and Responsibilities for a Peaceful, Safer and Rights Respecting Cyberspace*. We hope it will offer states, international organizations, industry, civil society, and other stakeholders a useful resource to support their efforts to stabilize and secure the online ecosystem.

The insights and ideas captured in these discussions and reported in this compendium reflect the diverse perspectives and expertise of a broad multistakeholder group, not necessarily the views of any one individual participant or the co-chairs of this project.

Contents

Foreword

Cyberspace has provided untold benefits and become an indispensable part of the daily lives of billions of people across the globe. At the same time, cybersecurity threats have become ubiquitous. Today, cyberattacks by state and non-state actors, including disruptions of critical infrastructure and government systems, large-scale thefts of data and intellectual property, election interference and other misinformation campaigns, are an all too regular occurrence. These incidents, moreover, cause significant harms to international peace and security, economic advancement, and human rights. Simply put, we are at risk of normalizing cyber insecurity.

However, this type of risk is hardly new. The 1996 Moonlight Maze incident,[1] which involved the theft of vast amounts of classified information from US government agencies and private sector entities, ushered in the current age of state sponsored cyberattacks. Today we are seeing crippling cyberattacks that shut down government services and raise the bar for concern. In Albania, a 2022 cyberattack temporarily shut down numerous government digital services and websites.[2] That same year in Ukraine, Russia's full-scale invasion shed light on their use of tools in a hybrid warfare strategy, including cyber weapons targeting government agencies.[3] In 2023, in Guam, Chinese threat actors targeted communications infrastructure, likely because it is a key strategic and logistical hub for US military operations in the Pacific.[4]

Fortunately, states and other stakeholders are not without tools to redress this rising insecurity. Rather than looking at cyberspace as some rule-free zone, existing international law can, and must, be integrated into the cyber context alongside the voluntary norms for responsible state behavior previously agreed in the United Nations (UN).[5] Today, the role of international law and norms are as widely recognized and established baselines for assessing state behavior online. As such, various nation states, non-state actors like the International Committee of the Red Cross (ICRC), and expert-driven processes (*e.g., the Tallinn Manuals and the Oxford Process*)[6] are now engaged in working to clarify how they do so.

Consistent with such efforts, the Ministry of Foreign Affairs of Mexico, Temple University's Institute for Law, Innovation & Technology (iLIT), and Microsoft have partnered to identify how to use international law and norms to make cyberspace more peaceful, safer, and rights-respecting. Our partnership reflects a shared commitment to advancing the application *and* efficacy of international law online while continuing to look for more bridges to increase state's capacity to leverage it. We are committed to doing so through a multistakeholder approach.

Through a series of three thematic workshops our project brought together foreign ministry representatives, international organization officials, international lawyers, civil society representatives, industry voices, and cybersecurity experts to identify lessons learned and good practices for employing international law in the cyber context. Importantly, we recognize that questions remain regarding the application and meaning of several key existing international law doctrines in cyberspace. These require continued attention from states and other stakeholders. At the same time, however, we believe that employing international law to regulate cyberspace cannot wait until some perfect consensus emerges.

1 **Forbes, Russia Has Carried Out 20-Years of Cyber Attacks That Call for International Response, 2020**

2 **Wired, An Attack on Albanian Government Suggests New Iranian Aggression, 2022**

3 **NPR, Russia bombards Ukraine with cyberattacks with limited impact, 2023**

4 **Microsoft Security Insider, Microsoft Digital Defense Report 2023 (MDDR), 2023**

5 See **Report of Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 (2015 GGE Report)**

6 See **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (cambridge.org)** and **The Oxford Process - Oxford Institute for Ethics, Law and Armed Conflict**

Rather, we believe that, alongside ongoing discussions on how to identify and interpret the various international law rules applicable in cyber contexts, there is ample room to explore opportunities to increase accountability under those rules and norms that already enjoy widespread support. In doing so, we look to complement existing efforts.

Key observations, proposals and good practices were developed as a concrete outcome from each workshop and formulated into the set of recommendations set out in this compendium. These aim to support the global community in efforts to ensure that international law's prohibitions, permissions, and requirements gain greater purchase with states and other stakeholders. Taken together, we believe that the recommendations contained in this *Multistakeholder Compendium on Advancing Opportunities and Responsibilities for a Peaceful, Safer and Rights Respecting Cyberspace* can facilitate states and other stakeholders applying international law to their own cyber operations, protecting human rights, and ensuring cyberspace is more peaceful and safer for people from all countries and communities.

Tom Burt
Corporate Vice President
Customer Security & Trust

Duncan B. Hollis
Laura H, Carnell Professor of law

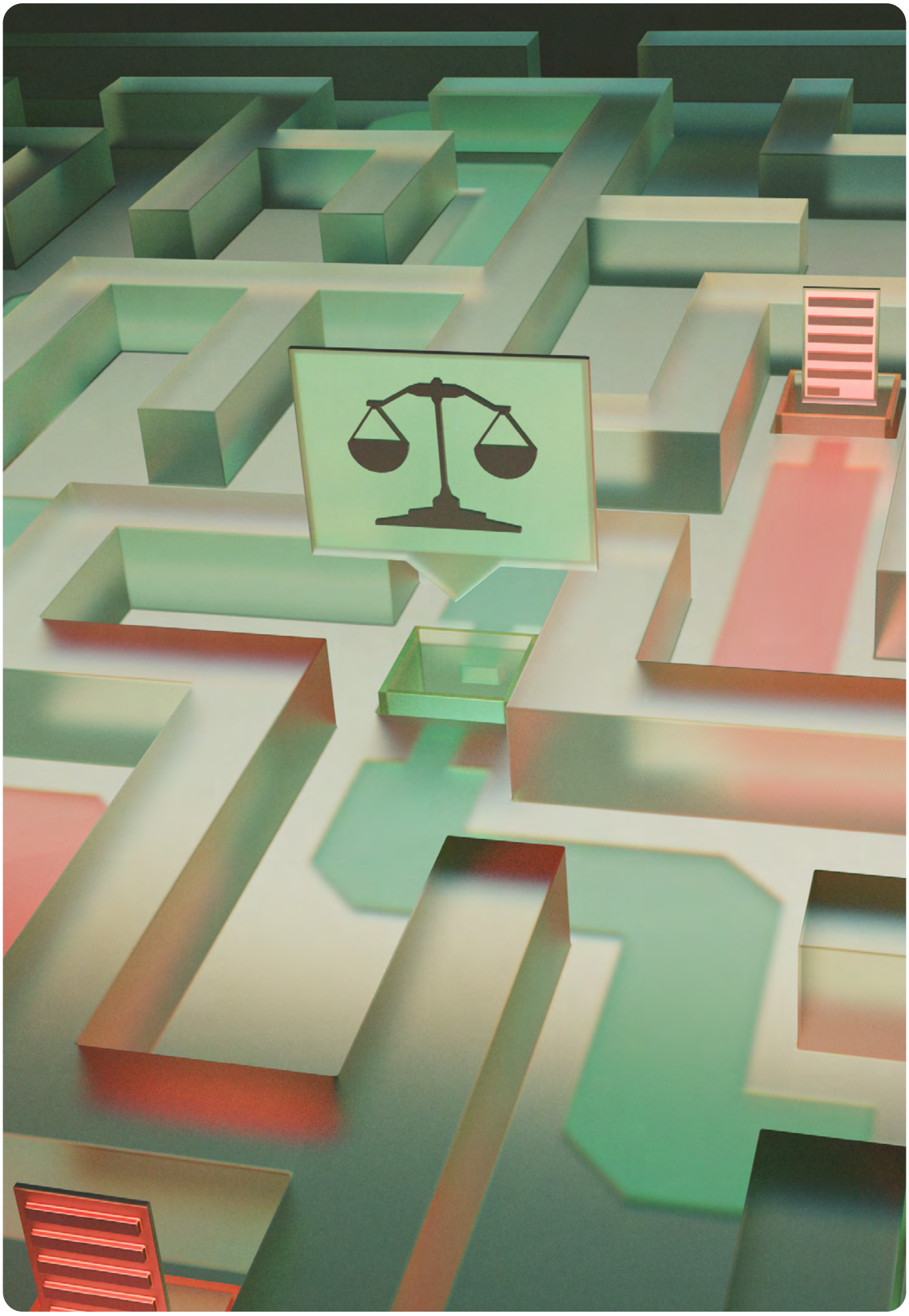
Dr. Eduardo Jaramillo Navarrete
Director General for the United Nations

Abygaelle Loubeau
Legal Fellow

Microsoft

Temple University
Beasley School of Law
Institute for Law, In
& Technology (iLIT)

RELACIONES EXTERIORES



Thematic workshop 1
Applying existing bodies of international law to cyberspace: successes and challenges

Cyberspace has increased opportunities for development for individuals, businesses, and nation states alike. However, it has also emerged as a distinct domain of conflict and competition among states. To effectively address this rising reality, there is a need to identify, clarify, and implement rights and obligations under international law in a manner that prioritizes human rights and protects people from reckless or malicious state behavior online. The first thematic workshop convened to advance this project.

During the workshop, panelists focused first on past successes in applying international law to cyberspace, acknowledging that too often these successes have gone under the radar. At the turn of the century, there were open questions about whether existing international law governed cyberspace at all or whether the novelty of the revolution in information and communication technologies (ICTs) meant cyberspace lacked international legal rules. All the panelists noted that states and other stakeholders have built a consensus that international law generally, and the UN Charter in particular, do apply to state behavior online. This was first affirmed by the 2013 Report of the UN Group of Governmental Experts (GGE), and affirmed in the 2015 GGE Report as well as 2021 Reports from the last UN GGE and the Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security (OEWG).[7] These conclusions have been noted by the UN General Assembly and endorsed in various regional international organizations and multilateral processes, such as ASEAN, the European Union, the Organization of American States (OAS), the G-7, and the G-20.[8]

Further successes were noted with respect to the question of how international law applies to cyberspace. In particular, participants highlighted the rising use of "national statements" by more than two dozen states to articulate how a wide array of international law doctrines operate in cyberspace.[9] Bodies within international organizations like the UN GGE and the OAS Inter-American Juridical Committee have facilitated such efforts, compiling various sets of national views and official responses to specific questions regarding international law

7 See **Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 (2013 GGE Report)** ("International law, and in particular the Charter of the United Nations, is applicable" to the ICT environment); **Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 (2015 GGE Report)**; **Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2021 (2021 GGE Report)**; **Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, 2021 (2021 OEWG Report**).

8 See, for example, **UN General Assembly Resolution 266, Jan. 2, 2019**; **OAS General Assembly Resolution 2959, Oct. 21, 2020**; **ASEAN-United States Leaders' Statement on Cybersecurity Cooperation, Nov. 18, 2018**; EU, **EU Statement – United Nations 1st Committee, Thematic Discussion on Other Disarmament Measures and International Security, Oct. 26, 2018**; **G7, G7 Declaration on Responsible States Behavior in Cyberspace, April 11, 2017**; **G20 Antalya Summit, Leader's Communique, Nov. 15-16, 2015, ¶26**.

9 For links and details on such statements see the online repository of national positions at **The Cyber Law Toolkit**: (national positions of **Australia (2020)**, **Brazil (2021)**, **Canada (2022)**, **China (2021)**, **Costa Rica (2023)**, **Czech Republic (2020)**, **Denmark (2023)**, Estonia (**2019** and **2021**), **Finland (2020)**, **France (2019)**, **Germany (2021)**, **Iran (2020)**, **Ireland (2023)**, **Israel (2020)**, **Italy (2021)**, **Japan (2021)**, **Kazakhstan (2021)**, **Kenya (2021)**, **Netherlands (2019)**, **New Zealand (2020)**, **Norway (2021)**, **Pakistan (2023)**, **Poland (2022)**, **Romania (2021)**, **Russia (2021)**, **Singapore (2021)**, **Sweden (2022)**, **Switzerland (2021)**, United Kingdom (**2018**, **2021** and **2022**), United States (**2012**, **2016**, **2020** and **2021**)).

in the cyber context.[10] The prospect of the African Union (AU) generating a common position on international law's applicability for all its Member States was highlighted in light of the ongoing work of the AU Commission on International Law.[11] The role of the International Committee of the Red Cross (ICRC) in cataloging and defending the application of international humanitarian law (IHL) to cyber operations in armed conflicts was also a subject of prominent attention. Several more academic projects received repeated mention as well, most notably the *Tallinn Manuals* (a comprehensive perspective that aims to deduce how existing international law doctrines analogize into the cyber context), the *CyberLaw Toolkit* (which uses hypotheticals to explore international law's operation in concrete ways), and The Oxford Process (which identifies what prohibitions, permissions, and requirements international law imposes on states with respect to certain specific objects of protection and methods of attack).[12]

Taken together, these efforts were praised for helping ensure more understanding as to where and what views on international law exist. It was emphasized that both identifying areas of emerging consensus as well as challenges understanding certain international law rules or principles, have value. Understanding where states and other stakeholders operate from a common position provides a useful foundation for identifying (i) the scope of the law's reach, (ii) non-conforming behavior, and (iii) the available vehicles to holding those responsible accountable. At the same time, greater visibility into where differences remain can establish an agenda for future dialogue around "grey areas." In the meantime, recognizing such divergences may help states and other stakeholders anticipate unaligned legal expectations with respect to certain cyber-operations with important implications for the (un)availability of some accountability mechanisms.

It was emphasized, however, that whatever value lies in appreciating existing successes, the framework needs improvement, especially in bringing more states into dialogue. That dialogue will necessarily invite further reflection on topics like (a) whether specific rules of international law applicable in other environments, like due diligence, are applicable to the cyber context; (b) how those rules that clearly do apply, like international humanitarian law (IHL), operate given the specificities of the online environment; (c) how to strengthen the mutually reinforcing nature of cyber norms and international law; (d) international law's treatment of non-state actors engaging in cyber operations during armed conflicts; and (e) the role of multistakeholder discussions and processes for advancing the operation of international law in cyberspace.

It is imperative that governments, industry, and civil society advance discussions on these questions to set and enforce clear boundaries that protect people online and promote confidence, transparency, and peaceful uses of cyberspace. Similarly, it is essential to explore whether the existing framework needs to be clarified, adjusted, or even amended in one or more ways.

10 See, for example, 2021 GGE Report, supra, **Official Compendium** (collecting national views from Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay); Duncan B. Hollis, **Fifth Report - International Law and State Cyber-operations: Improving Transparency**, Inter-American Juridical Committee, July 17, 2020 (surveying national responses to an OAS IAJC questionnaire from Bolivia, Brazil, Chile, Costa Rica, Ecuador, Guatemala, Guyana, Peru, and the United States); see also 2021 OEWG Report, supra, **¶38** (calling for more States to voluntary submit and share national positions).

11 **African Union, Press Release: The African Union Takes Significant Steps Towards Establishing a Common African Position on the Application of International Law in Cyberspace, June 30, 2023**

12 See **Michael Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber-operations (2nd ed., 2017)**; **Michael Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare (2013)**; **Compendium: The Oxford Process on International Law Protections in Cyberspace (2022)** (includes 5 "statements" each signed by over 100 international lawyers from across the globe on international law protections relating to healthcare, vaccine research, foreign election interference, information operations, and ransomware); **Cyberlaw Toolkit; Ewan Lawson and Kubo Mačák, ICRC Expert Meeting: Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts (Jan 2020)**; **Tilman Rodenhäuser and Mauro Vignati, "8 rules for 'civilian hackers' during war, and 4 obligations for states to restrain them," Humanitarian Law & Policy, ICRC, Oct. 4, 2023**. Meetings have also begun to compile a third edition of the Tallinn Manual.

Good practices, lessons learned, and recommendations identified by participants included:

- **States should continue leveraging past work at the United Nations and in various regional and multistakeholder fora in building consensus that international law currently governs cyber operations and other state behavior vis-à-vis cyberspace.** For states, the production of consensus reports are useful commodities. Past GGE reports and the annual OEWG progress reports therefore are extremely valuable evidence of state agreement and represent, in that sense, tangible progress. These efforts serve to demonstrate points of consensus that may build momentum in identifying additional areas of agreement. The level of specificity and detail in states' understanding and attention to these issues is much greater than it was even just a decade ago.

- **State and other stakeholders should include legal capacity building within broader capacity building efforts.** The UN GGE, the OEWG processes, and multistakeholder fora (e.g., the Global Forum on Cyber Expertise) have emphasized capacity building as a key pillar for ensuring cyberspace is open, secure, stable, accessible, and peaceful. Going forward, such efforts by states and other stakeholders should incorporate "legal capacity building" – efforts to inform lawyers of states and other stakeholders how international law and ICTs intersect, relevant areas of consensus and divergence, and any existing gaps so that those they advise can operate as informed and full-fledged participants in the operation of international law in cyberspace.

- **More states should offer additional views on international law's application to cyberspace.** To date, more than two dozen states have issued national statements on the application of international law to cyberspace. The topic is currently on the agenda of several regional international organizations giving their member states further opportunities to engage with questions of the law's applicability. Yet, most states remain silent on this topic, while those who do speak are often quite selective in what national positions they articulate. Recognizing that it is each state's prerogative as to when it makes its public views known and how it does so, we encourage more states to add their voices to the existing conversations and to invite those states that do speak to do so in more robust ways, further evidencing the state of customary international law, general principles, and other international legal rights and obligations that now govern states online. In any case, more attention is needed to the role of state silence in the cyber context, addressing questions such as whether or not a state's silence has any legal salience (such as acquiescence to other states' express interpretations of international law).

- **States should incorporate non-state voices into the dialogue over how to apply international law. States are the primary subjects and objects of international law.** In cyberspace, however, non-state actors own much of the underlying infrastructure. As such, it is important that as states aim to resolve the extant international legal rules, they consider whether and what roles ICT industry can play in understanding the relevant legal rules and facilitating accountability with their terms. Ideally, ICT companies and states can build common understandings on international law's application, which gaps exist, as well as other important differences requiring further dialogue and engagement. Individuals and firms have often suffered substantial and indiscriminate harms as a result of state and state-sponsored cyber operations. This harsh reality suggests states might do more to consider the victim's perspective in giving meaning to their IHL and international human rights law obligations in cyberspace.

- **States and other stakeholders should focus on areas of agreement and devise empirical methods to measure it.** There are areas where a convergence of views on the application of international law to cyberspace appear to exist (e.g., that the prohibitions on the use of force and intervention apply to cyber operations). They may provide a baseline against which to evaluate current compliance with international law and its efficacy. Moreover, other stakeholders in industry, academia, and civil society may develop and deploy empirical methods to discern these areas of convergence whether to identify a common interpretation of existing international law or the requisite general and uniform practice of states with

opinio juris to comprise cyber-specific customary international law. Here technologies such as big data analytics can be deployed to afford states and other stakeholders new (and perhaps more robust) methods to measure consensus, whether in terms of doctrines, areas of protection, or the means and methods permitted, prohibited or required of states online.

- **States' interpretation of existing international law should be expanded and is key to the law's success in governing cyberspace.** International law already contains several widely recognized general rules, principles, and standards that can speak to state behavior online. Thus, state-led processes for discerning how to interpret these international laws in cyber contexts will help determine if the law can be an effective vehicle for making cyberspace peaceful, safer, and rights-respecting. For example, even as states agree that coercive interventions are prohibited by international law, including by cyber means, it is still necessary for them to interpret which cyber behaviors comprise coercion (and which do not). In other words, it is not enough for states to know which rules of international law govern their behavior online but also when states are operating in conformity with those rules. Non-state actors can also play important roles in devising processes for interpretating and evaluating existing international law.

- **States should do more in discerning their positive obligations vis-à-vis cyberspace.** Much of the existing dialogue on international law and cyberspace has centered on its prohibitions - what states must not do online. But international law also includes positive obligations for states. For example, due diligence is a standard of state responsibility that manifests in various fields of international law, including (i) international human rights law, (ii) international humanitarian law, (iii) the no-harm principle, seen most prominently in international environmental law, and (iv) the *Corfu Channel* rule, which says that states must not allow their territory or jurisdiction to be the source of an abuse of another state's rights. States should work to balance the discourse to ensure equal attention to their negative and positive obligations, including most prominently to the way(s) due diligence operates on-line. Here too, non-state actors from the academy, industry, and civil society may help analyze and address the positive obligations states have in cyberspace.

- **States and other stakeholders should determine when and how private actors may trigger different international law frameworks.** International law generally focuses on regulating state behavior; only rarely do international legal obligations target individuals (e.g., prohibitions on terrorism, genocide). Yet, the frequency and severity of private actor cyber operations has implications for international law. Harmful cyber incidents could, for example, trigger state responsibility to remediate harms that occur in or transit their territory or jurisdiction under one or more versions of due diligence. Alternatively, private individuals may (individually or collectively) deploy ICTs in ways that entail those individuals' direct participation in armed hostilities, removing the protections IHL accords to civilians. Thus, even as the overall role of individuals as subjects of international law warrants attention, the issue is exacerbated online, warranting more focused attention from both states and other stakeholders alike.

- **States should ensure the protection of civilian data in armed conflicts.** Prohibiting direct attacks on civilian objects or disproportionately affecting them when attacking military objects are fundamental IHL principles. To date, however, states have not yet fully resolved if wiping civilian data, altering its contents, or denying access to it via cyber means could comprise an attack subject to these principles. Given the rising digitization of civilian data and the ways they are now targeted in armed conflict, states should consider having a more focused discussion of whether existing IHL regulates such operations and, if it does not, the relative costs and benefits of treating this as a gap in the law. While there is an increasing normative understanding that IHL does apply in cyberspace, constraining the potentially coercive actions of states in cyberspace requires states to further clarify how it applies.

- **States should give more attention to international law's human rights protections in cyberspace.** States have long agreed that the human rights available off-line require equal protections online. Yet, the precise contours of states' obligations to respect, protect, and ensure human rights remain underdeveloped in cyber contexts, to say nothing of where a state has such obligations. Hence, states should engage in further dialogue to identify the extraterritorial reach and substantive content of human rights online. Other actors may also add their voice to these conversations in order to make the idea of a human-centric approach a reality.

- **States and other stakeholders should continue to collaborate to create space for multistakeholder engagement on issues of international law's application to cyberspace.** Cyber threats by state and non-state actors may be described as a wicked problem – one requiring nuance and sophistication in responding and persistent attention in light of the dynamic quality of ICTs themselves. It is, moreover, a problem for which no single stakeholder group has sufficient capacity to address it entirely on their own. As such, states and other stakeholders would all benefit from one or more processes by which they could engage regularly on international legal questions.

- **Multistakeholder processes should complement state-led ones.** Rather than seeing existing state-led and multistakeholder projects on interpreting international law as competing, they should be viewed as complimentary efforts to explore and understand the law's capacity and authority in this space. It is important for states especially to recognize that circumstances may change over time given the rapidly shifting ICT environment. Hence, opinions on international law's application from a decade ago may have less relevance than more recent work.

Recommended readings and resources shared by participants:

- Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 28 May 2021
- The Cyber Law Toolkit
- Michael Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber-operations, 2nd ed., 2017
- The Oxford Process on International Law Protections in Cyberspace
- Duncan B. Hollis, Fifth Report, International Law and State Cyber-operations: Improving Transparency, Inter-American Juridical Committee of the Organization of American States, 17 July 2020
- ICRC, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions, 2022
- ICRC Global Advisory Board, Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to states, belligerents, tech companies, and humanitarian organizations, 2023
- T. Rodenhäuser and M. Vignati, 8 Rules for Civilian Hackers During War, and 4 Obligations for States to Restrain Them, EJIL:Talk!, 4 October 2023

Contributions by experts

The Distance Traveled in the Past Decade

It's been just over a decade that the law of cyber has been a subject of serious study in the legal academy. While it can sometimes feel like progress has been slow, it's worth stepping back to remember how far we have come in that time.

Just over a decade ago, there was significant debate over whether international law applied to cyber operations. Now we are in a different place. There is broad agreement that international law applies to cyber. There is broad agreement that states are not permitted to use force against one another through cyber means. There is broad agreement that states are not permitted to violate sovereignty through engaging in violations of the norm of non-intervention through cyber means. There is broad agreement that the law of armed conflict and human rights law and a range of other international laws apply to cyber operations. This may not seem like much, but it is a major step forward.

Of course, there remain areas of disagreement and thus there is much still to be done. There is disagreement, for example, over how, precisely, the principle of sovereignty applies to cyber. There is disagreement about whether there are obligations of due diligence and, if so, what they entail. There is disagreement about whether collective countermeasures are permitted and, if so, when and how. There is disagreement about how, precisely, to apply international humanitarian law to cyber. And there is disagreement about which cyber operations constitute violations of the prohibition on the use of force.

There are now conversations around the globe to continue to fill in the blanks and clarify the grey spaces. Some of the most important of these have been held through the Oxford Process. Progress can feel slow moving. It can be frustrating to see efforts through the United Nations come up short. But let's not lose sight of the distance we have traveled.

Oona Hathaway
Gerard C. and Bernice Latrobe Smith Professor of International Law
Yale Law School

Where are the successes and challenges in applying international law right now?

Since agreeing that existing international law applies in cyberspace in 2013, the international community has been focused on discussing its application. Even agreeing that international law applies was the result of detailed consideration of the matter by states, with significant contributions from academics and other organizations.

In the last few years, the UN Open-ended Working Group on cyber has built incrementally on the consensus that international law applies. States have gone from the proposition that international law, including the UN Charter, applies to recognising the application of specific articles and principles. These steps may seem minor but are significant in coming to a mutual understanding of what constitutes responsible state behaviour in cyberspace.

As the conversation builds, it is of fundamental importance that all states articulate their own views on the subject. The publication of national statements is not a mere academic exercise. States' national positions contribute in their own right to customary international law. Clarity, predictability and shared understandings of international law lower the risk of miscalculation and make clear the consequences of transgressing the rules. Having national positions to refer to go a long way towards this purpose.

The challenge before us is that much like other efforts to apply international law to particular scenarios,

there will be areas for debate. This notwithstanding, there is much further the international community can go in deepening its understanding of how international law applies in cyberspace. Initiatives, such as the workshops that underlie this compendium, are a valuable contribution to the conversation. This dialogue between states, as well as the broader stakeholder community, should itself be heralded a success.

Australia applauds the efforts taken by Mexico, Temple University and Microsoft for engaging states and the stakeholder community in this discussion, and we look forward to overcoming the challenges together.

Nish Perera
Legal adviser to the Australian Delegation to UN OEWG on Cyber
Department of Foreign Affairs and Trade

Successes and challenges in applying international law to cyberspace

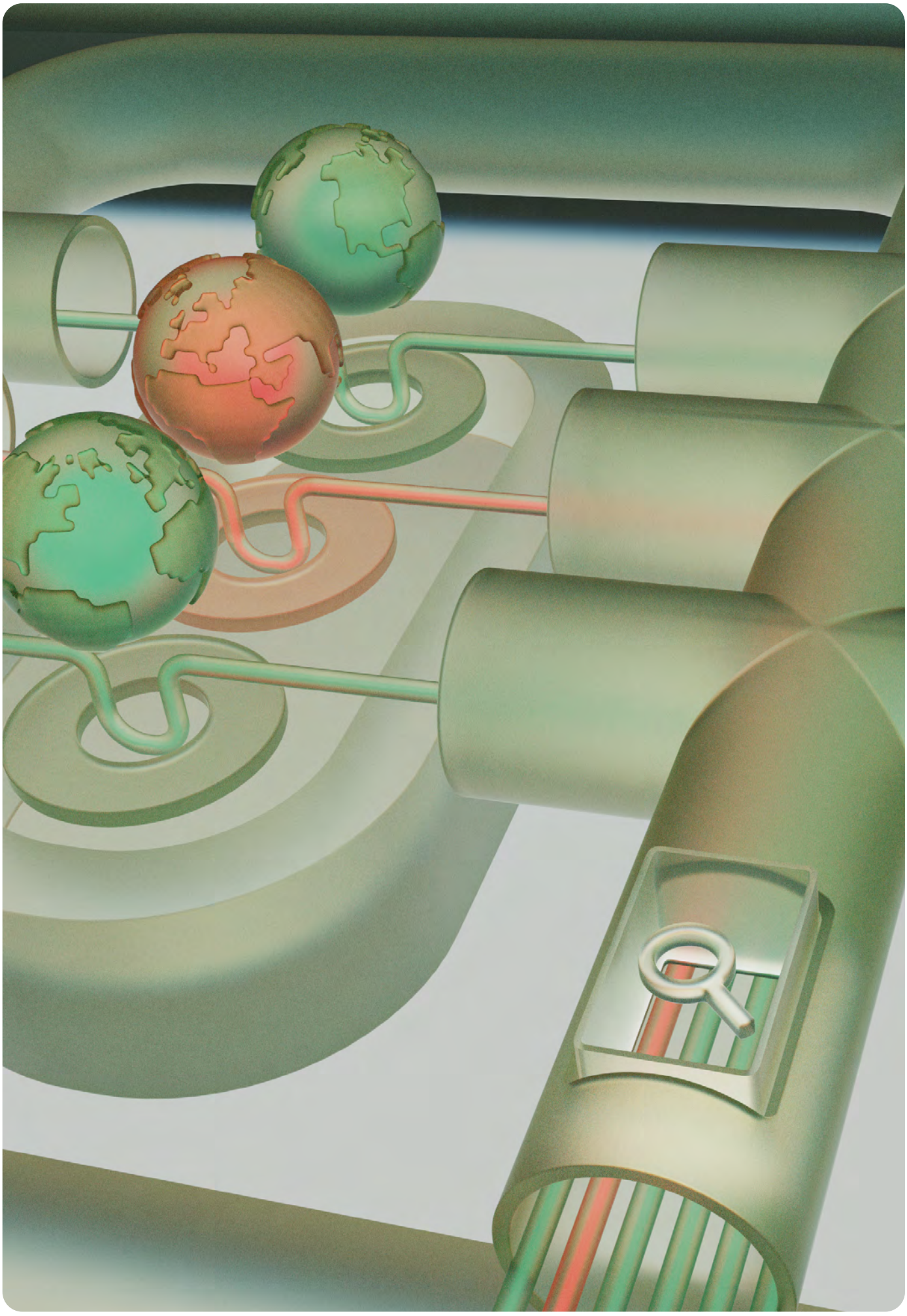
Over the past decade, there has been a significant evolution in discussions concerning the application of international law to cyberspace. Since 2013, when the UN Group of Governmental Experts (GGE) acknowledged the applicability of existing international law to state behavior in cyberspace and emphasized the relevance of the UN Charter within this context, the discourse has shifted from merely acknowledging the applicability to a more focused exploration of how international law applies, which we consider a significant success.

A notable recent achievement involves moving beyond general debates on the applicability of international law and delving into the specifics of how certain provisions, including principles such as sovereignty, due diligence, and non-intervention, are applicable. This shift towards substantive discussions is a significant milestone. Furthermore, the establishment of a roadmap during the ongoing Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security (OEWG) meetings, accompanied by the increasing participation of States, particularly those not traditionally participating in legal discussions, represents a key achievement.

On the other hand, these discussions have just taken their initial steps, and one of the foremost challenges lies in achieving consensus among the States on the exact application of international law and its principles. Such consensus would provide legal clarity, helping states to understand their rights and responsibilities in cyberspace. Another challenge in this process revolves around achieving consensus on the threshold for these principles.

To effectively address these issues, it is essential that the widest range of states engage in discussions regarding the applicability of existing international law to cyberspace, aiming to enhance and clarify the collective understanding of this complex domain.

Tereza Janáková
International Law Department
Ministry of Foreign Affairs of the Czech Republic



Thematic workshop 2
Improving state accountability for online behavior

As cyberspace has evolved into a new realm for enhancing human connections and communication, it has also given rise to new forms and magnitudes of harmful conduct. Regulating these behaviors has become an increasingly prominent concern for both states and various stakeholders. Consequently, there has been a growing effort to utilize existing international legal principles and obligations to address these challenges. Ongoing discussions persist regarding which specific branches of international law are applicable and how they should be applied, which was a central focus of the second workshop in this series.

In line with efforts to leverage existing international law to govern online behavior, states have reaffirmed the recognition and implementation of "voluntary norms of responsible state behavior." In 2015, the UN GGE delineated 11 such norms for adoption and implementation by states.[13] These norms have earned subsequent endorsements in the UN General Assembly, as well as in the final reports released in 2021 by the GGE and the OEWG on cybersecurity.[14] Simultaneously, various multistakeholder and expert-led initiatives, such as the Paris Call for Trust and Security in Cyberspace and the Global Commission on the Stability of Cyberspace, have also concentrated on identifying norms for online behavior.[15]

The second workshop focused on analyzing the character and utility of these normative efforts. It provided valuable insights into the importance of clarity in implementing the norms and the need to navigate complex issues like attribution and accountability for international law. Moreover, it explored how leveraging existing institutions and forums can help advance the understanding and implementation of international law in cyberspace. It also emphasized the importance of complementing existing discussions with creative approaches, fostering collaboration among diverse stakeholders, and understanding the interplay of norms and Confidence Building Measures (CBMs). On this topic, the significance of attribution, public-private cooperation, accountability, and preparedness were highlighted.

While consensus on the exact scope of international law's applicability remains elusive, norms offer a practical and constructive approach. By not imposing new obligations, but instead providing guidance on responsible state behavior in cyberspace, they facilitate a clearer understanding of expectations. They serve as a flexible framework that encourages cooperation, promotes peace, and lays the groundwork for more concrete developments in the realm of international law in cyberspace. This approach recognizes the evolving nature of the digital domain but at the same time allows for adaptation to emerging challenges and opportunities. However, one of the challenges identified during the workshop was the politicization of discussions around international law and voluntary norms in cyberspace. This political polarization has hindered the establishment of additional voluntary norms.

In cyberspace, attribution involves three layers of analysis: technical, legal, and political. The political layer, which considers the wider contextual factors, is where crucial decisions are made. Public attribution policies, as implemented by some countries, offer insights into the standards of proof used for attribution. The decision of whether to make an attribution public or private is a critical consideration and should be addressed through

13 **GGE Report, 2015**

14 **GGE Report 2021; OEWG Report, 2021**

15 See, for example, **Global Commission on Cyber Stability, Paris Call for Trust and Security in Cyberspace**

international policies. Participants also stressed the importance of examining the technical attributes of cyber operations. This includes understanding the scale, scope, and impact of these operations and their implications for international peace and security.

Accountability was recognized as a cornerstone concept in discussions on state responsibility. During the workshop, certain collegiate bodies were identified as potential bases for deep analysis on the application of international law in cyberspace, such as the International Law Commission.

One recommended future approach was to focus on the intersection of state behavior and the role of the private sector. Participants noted that private companies offer tools and services relevant to state behavior in cyberspace, particularly in the context of commercial spyware. This intersection aligns with discussions on state accountability and state responsibility (models like the UN guiding principles for business and human rights[16] or the US executive order for its National Cyber Security Strategy[17] were mentioned as potential guides for other governments).

The workshop emphasized the importance of leveraging existing institutions and forums rather than creating new ones. International law is applicable to cyberspace, and existing institutions, such as the UN Security Council, have been dedicating sessions to address cyber threats and challenges posed by cyberattacks. These sessions can be an ideal space to promote further debates and discussions. Utilizing such a fundamental basis, states can focus on recent developments and opportunities for further progress in the realm of international law and cyberspace governance.

Participants discussed the complexities associated with invoking specific principles of international law to hold an entire state accountable, as well as the jurisdictional power to hold individuals to account, which is primarily vested at the international level in institutions like the International Criminal Court. However, there are important implications to consider if a state official is found to be connected to a particular cyber operation or has engaged in hiring a private hacking group for example. These elements are intertwined and must be viewed holistically as practical approaches to addressing the issue.

Good practices, lessons learned, and recommendations identified by participants included:

- **States and other stakeholders should encourage creative initiatives that complement existing international discussions and aim to implement the agreed framework.** A growing number of cyber incidents pose a threat to national security. To address this, it is essential to complement ongoing international discussions at the UN level, with regional and subregional organizations that can be fertile grounds for innovative implementation strategies. One notable example[18] is the work that has been done via the OAS at the regional and sub-regional level to proactively promote stability in cyberspace.

- **States and all relevant stakeholders should foster global and regional information sharing and collaboration to enhance understanding and implementation of existing frameworks.** There is an overall need to enhance collaborative approaches involving governments, academia, researchers, civil society, and the private sector. There should be further disseminations of the pre-existing global and regional norms, CBMs, and relevant agreements related to cyberspace.

16 OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework

17 The White House, Executive Order on Improving the Nation's Cybersecurity, 2021

18 OAS Working group on cooperation and confidence-building measures in cyberspace

- **All stakeholders should promote a better understanding of the intricate relationship between norms and CBMs as mutually reinforcing elements in cyberspace.** The discussions revealed a critical insight – norms and CBMs must be considered in concert, rather than as separate silos. Thus, as new norms or the need for new norms are discussed in various UN and regional forums, it is important that states and other stakeholders assess how these norms can be complimented by CBMs.

- **States should further develop their concept of attribution as a crucial component to improve accountability and explore the interplay of its technical, legal, and political dimensions.** It was emphasized that attribution is a foundational pillar for applying international laws to cyberspace. Technical, legal, and political layers of analysis must converge to determine attribution, with the technical layer aiming to conduct factual investigations behind incidents.

- **States should encourage the creation of strategies to publicly address cyber incidents that violate international.** While many states have sought to identify those responsible for cyber incidents, few have taken the next step to declare such incidents as violations of international law. States should explore opportunities to make such declarations in the future. If attribution is a step that seems to obstruct doing so, regional models or common positions on international law in cyberspace might be a good basis to provide common baselines for future cases of attribution and accountability.

- **All relevant stakeholders should participate in promoting community awareness of state sponsored cyberattacks.** Alongside attributions related to international law, the significance of attribution for norm violations in cyber incidents, and publicly addressing these across stakeholder groups, was highlighted. Doing so can raise awareness beyond the traditional international peace and security discussions related to cyberspace.

- **States should embrace data-driven approaches to enhance accountability, including greater monitoring and analyses of cyber incidents.** Attribution is not the only option available for enhancing accountability and defending against cyber threats. States should also monitor attacks, measure their impact, and analyze violations of international law.

- **States can rely on the value of preparation as essential aspects of cybersecurity readiness.** The workshop highlighted the importance of preparedness to accountability, encompassing policy development, capacity building, and response plans for governments and organizations.

- **States can explore the development of a culture of compliance with international law in cyberspace.** States can foster a culture of compliance with international law in cyberspace through an instrumental commitment to responsible behavior. For example, engaging in the development of a national position on the applicability of international law in the digital domain, performing practical exercises with all relevant actors (e.g. table-top activities) and through constant cooperation among other states to build capacity in this key aspect at all levels.

- **The importance of all stakeholders in preserving a rules-based digital environment should be acknowledged.** Collaborative efforts that leverage the multilateral architecture that is already in place should be encouraged. Since each stakeholder has a unique role to play in defending cyberspace, it is key that multistakeholder platforms facilitate international cooperation. One concrete example is the Global Forum on Cyber Expertise (GFCE), which serves as platform where governments, international organizations, the private sector, academia, and civil society can come together to collaborate on various aspects of cybersecurity while providing a neutral space for dialogue and cooperation, information sharing, research, and norms development.

Recommended readings and resources shared by participants:

- United States National Cybersecurity Strategy, 2023
- European Union Cyber Resilience Act
- European Union Cyber Solidarity Act
- ORBIS, Due Diligence in Cyberspace - Guidelines for International and European Cyber Policy and Cybersecurity Policy, 2016
- UN Human Rights, Guiding Principles on Business and Human Rights, 2011
- Andraz Kastelic, UNIDIR, Non-Escalatory Attribution of International Cyber Incidents, 2022
- African Union, The African Union Takes Significant Steps Towards Establishing a Common African Position on the Application of International Law in Cyberspace, 2023
- OAS, Inter-American Juridical Committee, Second Report: International Law Applicable to Cyberspace, 2022
- Kristen Eichensehr, UCLA Law Review, The Law & Politics of Cyberattack Attribution, 2020
- The Global Forum on Cyber Expertise

Contributions by experts:

How does international law apply to state behavior in cyberspace just as it does to activities in other domains?

Cyberspace is not the Wild West; all countries have agreed that existing international law applies in cyberspace (GGE 2015) and all countries have endorsed UN norms of responsible state behavior.

International law, in particular the Charter of the United Nations, is applicable and fundamental to the maintenance of peace and stability and the promotion of peace and stability.

The reference to the Charter of the United Nations merely highlights one (if not the first) of the primary functions of the organization, which is to maintain international peace and security, and having that in mind, maintain an open, secure, peaceful and accessible environment in the field of these technologies.

The UN norms of responsible state behavior in cyberspace are 11 voluntary and non-binding rules that describe what states should and should not be doing in cyberspace. There is a way to help develop those rules of the road.

They express a common opinion of what is considered to be responsible behavior by states. Naturally, this collective opinion of what is responsible and what is irresponsible behavior develops over time as understanding of cybersecurity deepens, incidents occur, and more governments contribute to the process.

The purposes of the norms as reflected in UNGA Resolution 70/237 are to reduce risks to international peace and security, and to contribute to conflict prevention. They have been crafted to deal with state-to-state actions that could potentially carry the highest risks to international peace and security and the welfare of citizens.

Norms in international affairs are political agreements. They do not infringe on a state's sovereignty or impose legal obligations on states. In fact, the norms provide a common basis for a state to design strategic direction, develop capabilities and execute actions in a responsible manner.

Luis Serrano Molinos
Legal Advisor, International Law, Treaties and Legislative Affairs Division
Ministry of Foreign Affairs of Chile

Protecting civilians against fast-evolving cyber threats during armed conflict

In 1996, the International Court of Justice[19] famously held that international humanitarian law (IHL) applies 'to all forms of warfare and to all kinds of weapons', including 'those of the future'. Twenty-five years later, all States welcomed a report by a UN Group of Governmental Experts,[20] which agreed in the context of how international law applies to the use of Information and Communication Technologies (ICTs) by states that "international humanitarian law applies only in situations of armed conflict," and flagging that recalling IHL's application "by no means legitimizes or encourages conflict." Together with a growing number of national positions[21] on the subject, and in-depth discussions within states on the limits of cyber warfare, this is a significant success.

It is also generally agreed that further study is needed on how and when IHL applies to cyber operations. Two considerations are particularly important as States strive to find common understandings:

One, the long-standing rules of IHL only serve their purpose if applied in ways that ensure adequate protection for civilians, civilian infrastructure, and civilian data in our increasingly digitalized societies. Interpretations of IHL that focus on the protection of civilian objects against only physical damage are insufficient.

Two, we see a growing involvement of civilians – individuals, hacker groups, and companies – in cyber operations related to armed conflicts. The more civilians take part in these activities, and the more civilian infrastructure is used for military purposes, the greater the risk of civilians and civilian objects being targeted. The fast-evolving cyber threats to civilian populations require States to urgently find common understandings on legal boundaries. To inform such discussions, a global group of experts[22] – convened by the ICRC – recently presented four guiding principles and 25 recommendations to protect civilians against digital threats during armed conflicts.

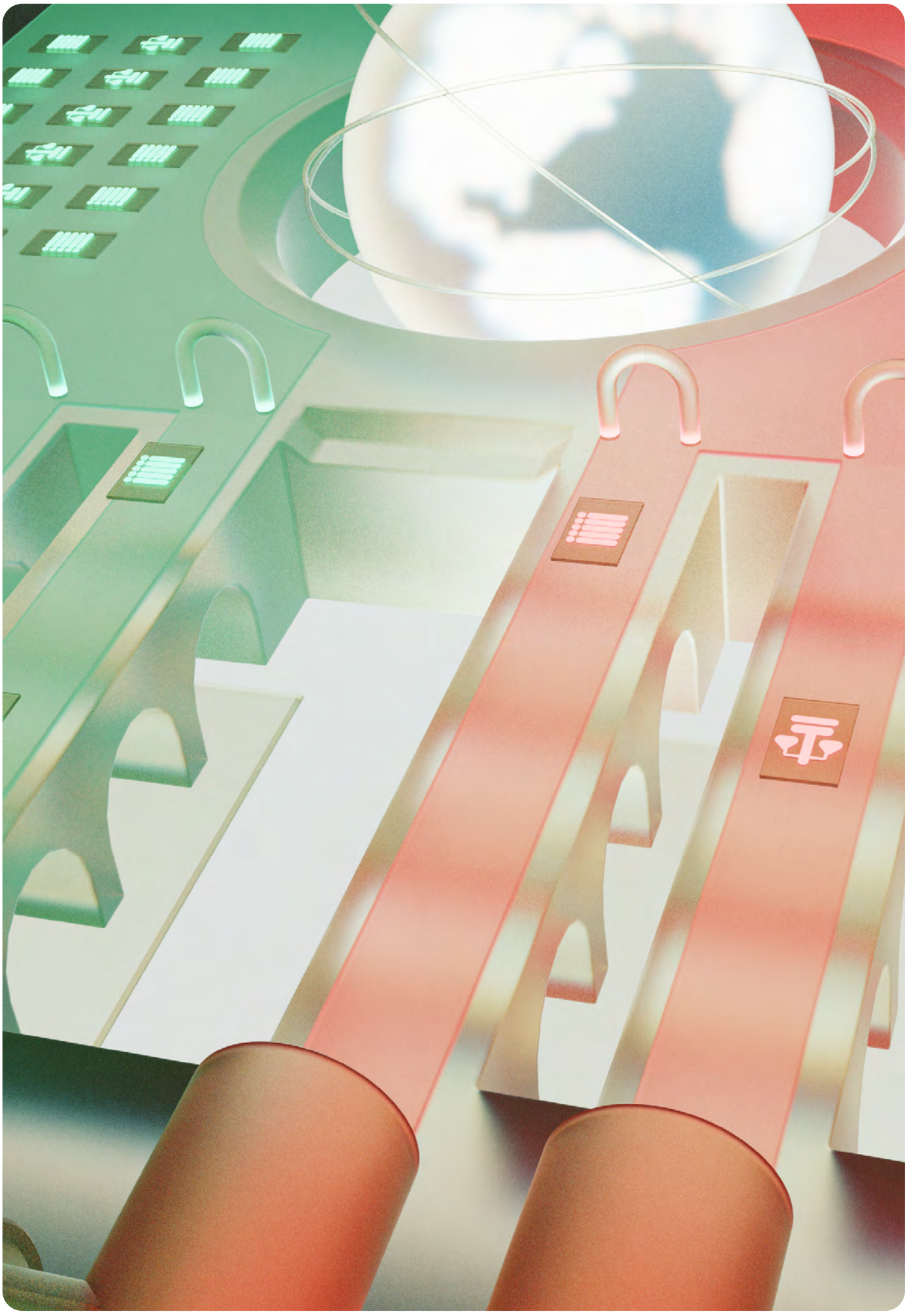
Dr. Tilman Rodenhäuser,
Legal Adviser,
International Committee of the Red Cross

19 **International Court of Justice, Legality of the Threat of Nuclear Weapons, Advisory Opinion, 1996**

20 **UN GGE Report, 2021**

21 **Cyberlaw Toolkit, National Positions**

22 **International Committee of the Red Cross (ICRC), Protecting Civilians Against Digital Threats During Armed Conflict, 2023**



Thematic workshop 3
Bridging digital gaps and promoting access to cyberspace

The digital age has revolutionized the way we communicate, work, and access information. However, as the world becomes increasingly interconnected, a significant portion of the global population still faces barriers to access the digital realm. Bridging digital gaps and ensuring access to cyberspace is a multifaceted challenge with multiple layers that involve a blend of technological, policy-related, and socioeconomic measures. To surmount this challenge several baseline capabilities, including international law capacity building, need to be considered and ultimately established.

In the context of this compendium, the training of state officials in international law was emphasized as being more important than ever. Multiple treaties reflect an expression of state agreement, but national level advancements could overlap and give rise to a complex set of obligations that are difficult to understand and implement. Unequal resources between states can give rise to disparities in capabilities exacerbating ongoing gaps in the implementation of international law.

During this workshop, it was emphasized that the digital divide is a pervasive issue that requires global, regional, and national engagement. The digital divide itself was characterized as disparities in access to digital technologies, the internet, and digital literacy which can impede international law capacity building. These disparities have far-reaching consequences, affecting not only individual opportunities but also broader aspects of society, including international security, economic development, and human rights.

One of the key components of bridging digital gaps is addressing technological barriers. Per the workshop, this entails not just expanding reliable digital infrastructure to reach remote and underserved areas, but empowering users to actively engage through meaningful digital inclusion and trainings based on global and comprehensive approaches for digital skills building. These should be regionally tailored to address both language and cultural differences and include capacity building at the national and international levels regarding the application of international law to the state use of ICTs. Initiatives to improve affordability, digital literacy, and the cybersecurity of digital infrastructure and users are also crucial in ensuring that individuals and communities can access and use digital resources effectively.

Harmonizing regulatory frameworks with international standards and norms can also create an environment conducive to digital access and innovation. The March 2021 UN OEWG consensus report affirmed the authority of international law in cyberspace and the set of norms for responsible behavior that were adopted as voluntary standards in 2015. It also encouraged states to be transparent and concrete about how they understand these rules apply and what they are doing to implement them. This leads to a capacity building need for both broader understandings of their applicability, and ultimately their implementation, with respect to international laws and the complimentary UN norms. The 2023 OEWG's second annual progress report[23] had a whole section dedicated to capacity building, which once again highlights the importance of this issue.

23 Open-Ended Working Group on security of and in the use of information and communications technologies, Second annual progress report, July 2023

However, states continue to have vastly different capabilities when it comes to conforming to these norms and laws, identifying, and responding to non-compliance by others, and contributing to a peaceful, safe, and rights-respecting cyberspace. As such, it was stressed that implementing international expectations in cyberspace will require identifying and filling foundational gaps across technical, political, legal contexts. Good practices, such as having institutions like Cyber Emergency Response Teams (CERTs), developing national cybersecurity strategies, conducting cybersecurity incident exercises, and increasing the capacity of states and stakeholders to contribute to broad accountability in cyberspace were discussed.

International law was addressed in this context as providing a guiding framework with principles that facilitate international cooperation in addressing the digital divide. These legal foundations not only serve as enablers of innovation, but also emphasize the need for accountable, responsible behavior in cyberspace. Moreover, the international human rights framework was discussed as being applicable to cyberspace, highlighting the importance of human rights in the digital realm. Advocating for capacity building efforts that promote digital inclusion should be guided by such human rights principles, ensuring that individuals can exercise their rights and freedoms online.

Acknowledging the existence of digital disparities and differentiated cyber capacities underscores the importance of multistakeholder collaboration as essential to steering states and other stakeholders in positive directions to build capacity. Governments, the private sector, academia, civil society, and citizens all have roles to play in ensuring equitable access to cyberspace and broadening the understanding of international law's applicability in cyberspace. Moreover, the broader community should not only map existing capacity building efforts that already exist but expand on what is already available.

As we shift to more practical ways of putting into practice the agreed norms and principles for the responsible and peaceful use of ICTs, it is important to find a balance between the developmental benefits of digital technologies and the potential security risks they may create. Providing recommendations to enhance capacities and finding ways to close digital gaps will significantly improve security and promote a wider understanding of state views on international law online.

Good practices, lessons learned, and recommendations identified by participants included:

- **All stakeholders must prioritize and work toward 'meaningful digital inclusion'.** This goes beyond working to provide infrastructure for connectivity and focusing as well on the quality, relevance, and impact of digital connectivity. Achieving full inclusion will require taking steps to resolve gender, regional, ethnic, urban-rural, and other divides within societies. Producing content, educational resources, and digital tools for commerce that are language inclusive and culturally attuned are important for bridging some of the deepest divides.

- **All relevant stakeholders working to implement norms through international working groups and similar processes should gather insights into the national contexts of norm declarations.** Normative declarations are often the result of political compromise at the national level. Understanding that context is key to developing action mechanisms that will be relevant, effective, and able to gain political and bureaucratic support within countries. This could lead to providing further clarity on applicability of international law in cyberspace, developing incident response plans and emergency management, and protection of critical infrastructure, to name a few capacity-building initiatives.

- **States should treat improving cybersecurity and international law capacity building as a development issue to leverage the full breadth of support possible from the multistakeholder community.** This will incentivize and enable greater participation by multilateral institutions, such as regional bodies, in capacity building at the national level. In parallel, this approach will help close digital divides both within and between countries and lead to the further study, discussion, and development of the application of international law to the state use of ICTs in the context of international security.

- **International organizations and civil society stakeholders should work to understand national and regional sensitivities around different capacity building efforts.** The historical trend of 'giving' capacity building programs to countries often produces limited success in long-term capacity building. Taking a more politically sensitive and demand-driven approach will help governments maintain political support for programs and engage the private sector to make commercially sustainable contributions.

- **States and relevant stakeholders should continue focusing on capacity-building efforts with the aim of ensuring that all states are able to participate on an equal footing on the development of common understandings on how international law applies in the use of ICTs.** Such capacity building efforts could include workshops, training courses, and exchanges on best practices at the international, inter-regional, regional and sub-regional levels, as well as draw from the experiences of relevant regional organizations, as appropriate.

- **All relevant stakeholders should focus their efforts on developing human-centric approaches to cybersecurity and international law.** The reliance of societies globally on digital technology means that both the understanding of cybersecurity threats, and the responses developed to address them, have ramifications for human rights and communities around the world and should therefore involve the engagement of a broad range of stakeholders. As such, stakeholders have a distinctive role to play in elucidating a human-centric understanding of cybersecurity and the applicability of international law within relevant policy forums. This also applies in implementing human-centric approaches to cyber norms developed and adopted within these forums. This recommendation is tied to access, for which an example that surfaced during the workshop was Mexico's 2013 amendments to Article 6 of their constitution making access to the internet a civil right.[24]

- **All relevant stakeholders should focus on international law capacity building as an essential part of improving cyber resilience.** Capacity building is a resource-intensive undertaking, which may be hard to prioritize in an under-resourced and overburdened context like cybersecurity. To overcome these challenges, the broader multistakeholder community can help map existing capacity building efforts centered on increasing the understanding of international law's application to cyberspace and expand on what is already available. Moreover, multistakeholder participation in identifying gaps in the existing legal framework and developing measures to advance accountability for cyberattacks is essential to advance international discussions on norms and improve overall cyber resilience.

- **States should avoid harmful provisions that may infringe on human rights and freedoms within legal and policy frameworks.** Existing (and future) legal and policy frameworks need to avoid overbroad, vague, and harmful provisions that may infringe on human rights and freedoms. Some of the common truths and myths that sometimes shape these frameworks, such as the tabula rasa argument, the moral panic argument, and the overemphasis on international law concepts of sovereignty and state authority should be avoided.

24 Freedom House, Mexico: Freedom in the World 2021 Country Report, 2021

Recommended readings and resources shared by participants:

- Robert Collett, *Understanding cybersecurity capacity building and its relationship to norms and confidence building measures*, Journal of Cyber Policy, 2021
- Global Conference on Cyber Capacity Building (GC3B), Global Forum on Cyber Expertise (GFCE), November 2023
- International Telecommunication Union (ITU), National Strategies
- Chris Painter, *Building an International Cybersecurity Regime, Multistakeholder Diplomacy*, Chapter 6, Edward Elgar Publishing, 2023
- Freedom House, *Mexico: Freedom in the World 2021 Country Report*, 2021

Contributions by experts:

Realizing a human-centric approach through inclusive cyber norm policymaking

Global Partners Digital (GPD) is a civil society and human rights organization. Specifically, the work we do is about ensuring the governance of digital technology–frameworks, norms and standards relating to digital technology–are rights respecting and inclusive of all stakeholders, including those most adversely impacted. This includes the governance of cybersecurity and specifically the framework of responsible state behavior in cyberspace.

In our work, we emphasize the importance of a human-centric approach to the governance of cybersecurity and to the implementation of the norms and principles for responsible state behavior. At its core, a human-centric approach makes the human being the central referent by placing human needs and well-being at the center of policymaking and implementation. It emphasizes the value of international human rights law as a guiding framework from which the norms and principles are derived from or related to. This includes recognizing the need to address the digital divide through meaningful and secure access to digital technologies for all.

A foundational gap we have encountered in our work is a lack of understanding of how a human-centric approach is applied in practice. To contribute to fostering a shared understanding of what human-centric implementation means, GPD recently published the "Inclusive Cyber Norms Toolkit"[25] with practical and action-oriented guidance on considering inclusivity in norm development and implementation through policymaking processes.[26] The Toolkit aims to help actualize a human-centric approach by making the needs and wellbeing of those whose rights are most adversely affected in cyberspace a central referent within relevant policymaking processes.

For example, efforts to bridge the digital divide must be inclusive and engage marginalized groups to be human-centric. The Toolkit's purpose is to ensure the most impacted individuals or groups shape the translation of the norms and principles through initiatives and policies which benefit them.

Global Partners Digital

What Happens in Cyberspace Will Not Stay in Cyberspace

It is essential for Africa to become actively engaged in the debates on international law and cyberspace. This debate is too important and the stakes are too high for Africa to remain silent in this conversation. There are two reasons – political and legal – that make it imperative for us to ensure that Africa's voice is heard in the process of articulating the rules of international law that govern cyberspace. The first reason – which is political – is obvious. Cyberspace

25 See Inclusive Cyber Norms Toolkit – Global Partners Digital (gp-digital.org)

26 See, for example, Myriam Dunn Cavelty, Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities, Science and Engineering Ethics, 2014

is ubiquitous. It penetrates every aspect of our lives. Cyberspace is also an indispensable vehicle for sustainable development, especially in Africa. The overarching policy objective for Africa must be to ensure that cyberspace is peaceful, safe, stable and open, which supports our efforts to realize the ambitious goals that are laid-out in Africa's Digital Transformation Strategy. One of the core objectives of this strategy is to "break the digital divide", which is a multifaceted phenomenon that includes technical, infrastructural, gender, and political aspects. Addressing the digital divide requires keeping cyberspace safe and secure, which is essential for promoting inclusive economic growth and advancing the cause of Pan-African integration.

From a legal perspective, it is important that Africa becomes active in debates on the legal regulation of cyberspace. These global conversations have the potential to reshape the architecture of international law. The advent of cyberspace is challenging many foundational principles of international law. Debates in this field will have a systemic effect on the architecture of international law. In short, what happens in cyberspace will not stay in cyberspace. If Africa's voice continues to be missing from this conversation, we may find ourselves bound to rules and regimes that regulate cyberspace that evolved without our participation. Our silence could amount to acquiescence and our failure to influence the normative trajectory in this field may undermine our rights, interests, and security. That is why the African Union is working to articulate a Common African Position on international law and cyberspace, which hopefully will make a constructive contribution to global conversations in this field.

Mohamed S. Helal
Professor,
Ohio State Moritz College of Law & African Union Special Rapporteur
on the Application of International Law in Cyberspace

Multistakeholder Capacity Building as a Foundation for Global Cyber Stability

Against a backdrop of ever-increasing threats in cyberspace and the great promise that digital economies can bring to both developed and developing countries, it is clear that lesser developed countries are at risk of being left further behind if there is not concerted action to help them build needed cybersecurity capabilities and policies. Cybersecurity capacity building is foundational both to countering all the malicious actions and actors in cyberspace, but also to realizing the significant benefits that cyberspace offers to future economic and social development. Yet, the demand for cyber capacity building greatly outstrips the resources and priority devoted to this endeavor.

A multistakeholder and multiregional approach is required to adequately meet this urgent demand. Although there has been much debate about the role of non-state stakeholders in various aspects of cyber policy, the consensus reached in the first OEWG final report in 2021 made clear that all stakeholders have a vital role in ensuring cyber capacity building as a necessary predicate to countries being able to defend themselves from cyberattack, participate in cyber policy discussions and safeguard their infrastructure.

The Global Forum on Cyber Expertise (GFCE) is an answer to this call and is a fully multistakeholder organization – comprised of states, the private sector and civil society – designed to promote cyber capacity building both globally and regionally. It employs a "demand-driven" approach to ensure that capacity building is sustainable and effective. Through its global Cybil Portal,[27] it provides an extensive information sharing platform and through its several recently launched regional hubs it aims to make sure capacity building is grounded in local realities. Critically, the GFCE also seeks to break down existing stovepipes and bring important communities of interest together – including the cybersecurity capacity building and the traditional development community. As partners to the government of Ghana, the GFCE, World Bank, World Economic Forum, and CyberPeace Institute held the first high-level Global Conference on Cyber Capacity Building and released the Accra Call for Cyber resilient Development[28] that is a multistakeholder action framework for concrete progress on this important foundational issue.

Christopher Painter
President,
Global Forum on Cyber Expertise (GFCE) Foundation Board

27 See Homepage - Cybil Portal

28 See Global Conference On Cyber Capacity Building GC3B – Global Conference On Cyber Capacity Building

Microsoft

Temple University
Beasley School of Law

Institute for Law, In
& Technology (iLIT)

RELACIONES EXTERIORES
SECRETARÍA DE RELACIONES EXTERIORES