Advancing Accountability in Cyberspace
Models, Mechanisms, and Multistakeholder Approaches

Edited by Allison Pytlak and James Siebens
ABOUT STIMSON

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

Contributors

Anne-Marie Buzatu, Executive Director, ICT4Peace Foundation
Rosa Celorio, Associate Dean for International and Comparative Legal Studies & Burnett Family Distinguished Professorial Lecturer in International and Comparative Law and Policy, George Washington University
Debra Decker, Senior Advisor, Cyber, Stimson Center
Reece Iriye, 2023-2024 Tower Scholar, Southern Methodist University
Shreya Lad, Research Assistant, Cyber, Stimson Center
Moliehi Makumane, Researcher, Security and Technology Programme, United Nations Institute for Disarmament Research (UNIDIR)
Zhanna L. Malekos Smith, JD, Senior Associate (Non-resident), Aerospace Security Project, and Adjunct Fellow (Non-resident), Strategic Technologies Program, Center for Strategic and International Studies (CSIS); Visiting Fellow, Carnegie Council; Cyber Law and Policy Fellow, Army Cyber Institute, U.S. Military Academy at West Point
Allison Pytlak, Program Lead, Cyber, Stimson Center
Kathryn Rauhut, Nonresident Fellow, Cyber, Stimson Center
James A. Siebens, Fellow, Cyber, and Project Lead, Defense Strategy & Planning, Stimson Center

All views expressed by individual contributors are their own, and do not reflect those of their organizations or affiliates.

Please Cite this Publication As


Acknowledgements

We would like to thank the following individuals for their diverse contributions and support to this report, through peer review, informal interviews, and participation in our workshops and events: Janine Alder, Sabrina Alvarez, Lise Andersen, Denia Baikari, Christopher Barclay, Jérôme Barbier, Vincent Barras, Kerry Ann Barrett, Tina Birmpili, Jeffrey D. Bean, Mark Bromley, Andrea Calderaro, Ella Carlberg, Scott Cooper, Amb. Martin Dahinden (retired), J. Michael Daniel, Heather Dresser, Charles Eberle, Isabel Ebert, David Fairchild, Agathe Favetto, Sheila Flynn, Jerry Gupta, Sherif Hashem, Osin Herbots, Sean Heritage, Marie Humeau, 1LT Christina Huynh, 1LT Nicholas H. Kacavas, Piotr Kijewski, Daniel Klingele, Cadet Christopher T. Konin, Amb. Timo S. Koster (retired), Sheetal Kumar, Peter Kvist, Thomas Larsen, Cadet Conner R. Leggett, Marc Limon, Anders Lindell, Lt. Col. Katherine C. Mack (USAF), Cadet Cole McKee, Bruce McConnell, Ellie McDonald, Isaac Morales, Diego Sanchez Moreno, Darren Pain, Chris Painter, Pavlina Pavlova, Patryk Pawlak, Benjamin Perren, Clare Perry, Giacomo Persi Paoli, Kimberley Raleigh, Christian Ranger, MacKenna Rawlins, Monica Ruiz, Andrea Salvi, Alizee Semon, Max Smeets, Christoph Sommers, Sorina Teleanu, Oceane Theriot, Michael Teodori, Correlli Van Hulten; the International Telecommunications Union (ITU) Telecommunications Development Bureau (BDT) Cybersecurity Division; and the Washington Foreign Law Society.

Special thanks are due to the EU Institute for Security Studies and its EU Cyber Direct Project for their collaboration and in-kind support. We wish to acknowledge the authors of a series of shorter papers on cyber accountability that have been published jointly with the EU Cyber Direct as part of this project: Andrea Calderaro, Cardiff University; Taylor Grossman, Institute for Security and Technology; Louise Marie Hurel, Royal United Services Institute; Moliehi Makumane, UN Institute for Disarmament Research; and Martin Alexander Muller, University of Innsbruck.

This report was made possible through the support of the Governments of Canada and Switzerland, and Peraton.
Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches

Edited by Allison Pytlak and James Siebens
Contents

1. Introduction ....................................................................................................................................... 5
Understanding Accountability and Deterrence .................................................................................. 6
Approaches to Cyber Accountability ................................................................................................. 9
Research Methodology and Report Overview .................................................................................. 9

2. Reimagining Cyber Arms Control .................................................................................................. 15
Introduction ........................................................................................................................................ 15
Cyber, Arms Control, and Nonproliferation ....................................................................................... 15
Case Study 1: The Arms Trade Treaty ............................................................................................. 18
Case Study 2: The Wassenaar Arrangement ....................................................................................... 23
Relevance to Cyber .......................................................................................................................... 25
Key Takeaways and Recommendations .......................................................................................... 28

3. The Implementation of UN Security Council Resolution 1540 ................................................ 34
Introduction ........................................................................................................................................ 34
Developing Review and Assessment Mechanisms for Accountability ............................................. 35
Key Takeaways and Recommendations .......................................................................................... 40

4. Is there a Space Skeleton Key for Unlocking Accountability in Cyberspace? .............................. 46
Outer Space Governance .................................................................................................................. 46
Case Study 1: The Artemis Accords’ Principles and Lunar Program .............................................. 47
Case Study 2: Promoting Accountability Via Capacity-Building ..................................................... 51
Key Takeaways and Recommendations .......................................................................................... 53

5. The Remarkable Story of the Montreal Protocol with Lessons for Cyberspace ......................... 57
An Evolving Framework .................................................................................................................... 57
Overseeing and Incentivizing Compliance ........................................................................................ 59
Key Factors in the Development of the Agreement and Its Mechanisms ...................................... 60
Relevance to Cyber .......................................................................................................................... 63
Key Takeaways and Recommendations .......................................................................................... 63

6. The Cyber World and Human Rights: Perspectives on International Accountability ............... 70
Introduction: Human Rights and Digital Spaces .............................................................................. 70
Connection Between Human Rights Concerns and Cyberspace ................................................... 71
Key Takeaways and Recommendations .......................................................................................... 73
1. Introduction

Allison Pytlak and James Siebens

The cyber domain presents unique and daunting challenges for policymakers seeking to reduce threats and avoid harms caused by malicious cyber activity. Cyber threats are both persistent and omnipresent, as the technical capabilities and the tools required to generate cyber threats are widely available, and access to them is difficult (if not impossible) to strictly control. Malicious cyber activities have thus proven difficult to manage through traditional approaches to deterrence, arms control, or law enforcement. Despite the challenges with addressing cyber threats with traditional security tools, the dangers emanating from malicious cyber activities can produce significant real-world harms for private individuals, businesses, organizations, and governments alike. In extreme cases, they present risks of severe disruptions to critical infrastructure or security systems that have the potential to escalate into major international crises, and even armed conflict.

Unfortunately, progress in implementing behavioral norms and understanding how States interpret existing international law as applying to cyberspace has been slow and uneven. As a result, calls for accountability are growing, most notably from UN Secretary-General Antonio Guterres. In 2023 he recommended the establishment of “…an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct. This mechanism could enhance compliance with agreed norms and principles of responsible State behaviour.”

To help deter such incidents and reduce the risk of catastrophic events, already accepted international norms and law need to be more effectively implemented, and further international cooperation and coordination is needed to support a system of greater accountability. Accountability and liability for violations of norms and law are a critical part of implementation, and concern states seeking to address and deter malign behaviors, as well as private victims of malicious cyber activities who might seek restitution for harms caused by malicious cyber actors.

Since 2022, Stimson’s Cyber Program has been researching the implementation of international norms and law in other international threat areas—for example, conventional arms control; the regulation of chemical, biological, radiological, and nuclear materials; management of the private military and security industry; and military uses of outer space, to cite a few examples. It has also examined various dimensions of cyber accountability through a webinar series, in-person convenings and events, and a collaboration with the EU Institute for Security Studies (EU ISS). For more about the Stimson Center’s Cyber Accountability project, please visit our website.

The primary purpose of our work over the past two years has been to draw out lessons about how transnational threats have been managed in these other issue areas—especially through the establishment
of accountability mechanisms that help shape incentive structures to encourage good practices and
discourage harmful or proscribed behaviors—that may be appropriately adapted or applied to the cyber
domain. This report is thus intended to provide policymakers and other stakeholders in the cyber
community with a “toolkit” of policy approaches that have already been tried and tested in other contexts,
and to offer potential pragmatic paths forward to enhance accountability in the cyber domain, and thereby
improve deterrence of malicious cyber activities.

Understanding Accountability and Deterrence

This report is focused on the concept of accountability and how it might be applied to malicious activity
in cyberspace to create more positive incentive structures and better deter dangerous, disruptive, and
destructive behaviors.²

The concept of cyber accountability or rather, interest in how accountability might be strengthened in the
cyber policy domain has been steadily growing in recent years. Various scholars and policy experts have
contributed to a growing body of literature on the topic, at times in relation to concepts of transparency
and responsible behavior.³ Much of this research builds on other efforts to strengthen awareness and
understanding of agreed behavioral norms and the applicability of international law to cyberspace.
Understandably, research and dialogue about cyber accountability has often included consideration of
cyber attribution, whether that is technical, legal, or political.

The 11 voluntary norms for Responsible State Behavior in Cyberspace were developed by the 2015 UN Group of
Governmental Experts. Image by Australian Strategic Policy Institute (ASPI).
Along with the eleven UN norms, collective capacity-building, confidence-building measures, and adherence to obligations under international law form the UN framework for responsible behavior in cyberspace. Illustration by ASPI, the UN General Assembly, and the U.S. Department of State Bureau of Cyberspace and Digital Policy.

In cyberspace, behavioral norms stem from existing state obligations under international law, as well as collective and national interpretations on the application of international law. In 2013, a UN Group of Governmental Experts (GGE) agreed that international law is applicable to state conduct in the use of information and communications technology (ICT). In 2015, a subsequent GGE outlined and adopted a set of 11 non-binding, voluntary norms for state behavior focused on peacetime use of ICTs. The applicability of international law and the norms have been repeatedly endorsed by the entirety of the UN membership through UN General Assembly resolutions. International law and norms, coupled with confidence building measures and underpinned by cyber capacity-building, is increasingly being referred to by diplomats, policymakers, and others as the UN Framework for Responsible Behavior in Cyberspace (hereafter, the Framework). Yet there are other relevant foundations for assessing accountability, including laws on cybercrime, national cyber security strategies, and regional policies or frameworks.

In international relations, accountability is usually viewed through a state-centric lens, as the ability to enforce norms, standards, or rules among and within states by attributing responsibility for undesirable behaviors. It is perhaps most often interpreted in this negative form—enforcing rules by imposing costs, seeking to prevent “bad” behavior through the threat of consequences. As such, it is seen as a capacity
that states possess to enforce a set of rules within their own borders through law enforcement; or against one another, typically through diplomatic, economic, or military means.

This type of negative accountability has generally been the preferred model in cyberspace. Negative accountability in the cyber context refers to obligations by actors (usually states) to refrain from malicious actions that would violate agreed norms, and to collectively punish such violations by imposing costs and consequences on the perpetrator(s). This definition also features in the way state actors understand accountability and implement it through national cyber strategies. This conception of accountability is closely related to the concept of deterrence, which relies on the credible threat of imposing costs on those who engage in proscribed behaviors, such that the anticipated costs of the action outweigh the potential benefits. Proponents of negative accountability argue that the most effective way for norms to have effect on shaping behavior is by reliably imposing consequences on those who carry out unlawful or proscribed actions in cyberspace. This has meant that attribution, or the practice of identifying and assigning responsibility to the source and perpetrator of a network intrusion, exploit, or attack in cyberspace, has been the emphasis of most accountability models in cyberspace. Thus, sustained engagement through voluntary collective action is key to ensuring that consequences for any violations of can be credibly threatened and, if necessary, effectively imposed, with the goal being to achieve deterrence through accountability in the cyber domain.

However, for a variety of reasons, malicious cyber activities have proven especially difficult to deter. Firstly, it is sometimes difficult to determine exactly who is responsible for carrying out malicious cyber actions due to the technical sophistication of the malign actor, or the limited technical capabilities of their intended target(s). Secondly, even in cases where strong technical attribution is possible, the victim(s) may not have the capabilities necessary to impose sufficient costs on the perpetrator(s), or they may be unwilling to do so (or even to make an attribution) based on political considerations. Further, there may not be adequate international agreement on the legal process by which criminal charges or civil suits can be brought, or the standards of evidence to be presented against the alleged perpetrator(s), making it difficult to pursue legal remedy reliably or effectively for harms caused by malicious cyber activities. The above complications, as well as the inherently covert nature of cyber activity and capabilities, have contributed to widespread rejection of cyber deterrence as a salient and relevant model.

Scholars have also found it useful to theorize accountability as a power relationship whereby a power-wielding actor is accountable to another actor who constrains the powers and decisions of the former, such as an elected official and the electorate. Both power wielders and accountability holders can be states, non-state actors, or international and commercial organizations. This understanding of accountability positions it in the context of a subject and object of accountability, accountability held by ‘whom,’ and ‘to whom.’ This helps give credence to understanding accountability its positive sense: being answerable for fulfilling an obligation, such as actions or policies that must be enacted and upheld to maintain cyber resilience. Strong defenses against harmful or destabilizing actions can reduce the benefits a malicious actor can expect to gain from such an act and make it costlier for malicious actors to conduct harmful cyber operations. Cyber capacity-building (CCB) can make digital systems and supply chains more resilient in anticipation of attacks or intrusions, and signal to adversaries or threat actors the costs of engaging in such acts.

Broader acceptance of a positive accountability lens might offer a promising direction for deterrence through mechanisms for accountability. By building resilience through positive obligations that actors can
voluntarily abide by, supported by a set of incentive structures, and developed with multiple stakeholders in mind, the international community as a whole can deter undesirable or disruptive outcomes in specific contexts or use-cases in the cyber domain. Cyberspace is a domain with multiple stakeholders, including states, intergovernmental organizations, multinational corporations, nongovernmental organizations, and even private individuals and groups that operate internationally, and is thus inherently complex. It therefore requires a pluralistic and multi-dimensional approach that goes beyond accountability in the negative sense of enforcing rules by imposing costs.\(^\text{12}\)

**Approaches to Cyber Accountability**

This leads back to the initial premise of this report in which cyber deterrence is reimagined and repurposed through an accountability lens. Our research considers both forms of accountability in a broader context of global cyber governance and the full ecosystem of actors involved: national governments, international and intergovernmental organizations, the private sector, law enforcement, civil society, and researchers.

While cyberspace possesses unique characteristics, the malicious and strategic use of ICT can also be understood as yet another threat domain posing security challenges and risks. Approaches to managing its threats and risks are can therefore be informed by experiences from other transnational threats, from conventional weapons to weapons of mass destruction (WMD) to chlorofluorocarbons. Formal and informal mechanisms exist ranging from diplomatic pressure to sanctions and prosecutions to military actions for holding states and individuals accountable for actions that harm or could cause harm, and for developing networks/expertise to continually improve these mechanisms. Although some work has been undertaken to promote cyber norms’ implementation and to progress accountability, there are very few lessons-learned examinations of cases in other domains and application of these lessons to cyberspace that could progress efforts.

**Research Methodology and Report Overview**

The initial phase of this research project sought to identify areas that have some level of international cooperation around managing risk through establishing norms of behavior and models of accountability that might offer useful analogies to the challenges faced in the cyber domain. A critical consideration for case selection was whether the area under consideration had similar governance challenges to cyber, such as difficulties in attribution, accountability, liability, and reliable consequences; or if it has similar characteristics such as a diversity of actors, including governmental and nongovernmental, with disparate interests, varied risks, and cross-domain intersectionality.

After an initial review of more than 30 different transnational security challenges and/or issue areas, the following issues were selected for further research through case studies designed to identify potentially useful analogies, lessons, and models which may be instructive for advancing accountability and addressing challenges in cyber diplomacy and governance.

In Chapter 2, Allison Pytlak outlines the extant literature on arms control and nonproliferation. She highlights the main contours of a longstanding debate amongst academics and policymakers on the feasibility of applying traditional arms control and nonproliferation approaches to international cyber security.
Pytlak offers two studies of conventional arms control mechanisms—the Arms Trade Treaty and the Wassenaar Arrangement—and presents lessons from both mechanisms. A key point from the analysis is the importance of focusing on the regulation of behavior and activity rather than specific technologies. In both instances, Pytlak highlights the importance of incentives for compliance, and points to the need to revisit the concept of dual-use for a cyber and digital context. She concludes that a toolbox approach of formal and informal mechanisms, and tools, will enable policy and regulatory responses that are more focused on specific cyber threats and challenges.

Continuing with the theme of arms control and nonproliferation, in Chapter 3 Debra Decker and Kathryn Rauhut examine UN Security Council Resolution 1540 and its related Matrices. While the risks from WMD nonproliferation regimes are addressed in other treaties and agreements, they were not universally adopted and did not cover all security risks; UNSCR 1540 closed those gaps. Decker and Rauhut explain how the 1540 Matrices have helped countries better understand their obligations and posit that comprehensive and independent risk assessments would help to provide consistent metrics and guidance to policymakers. To that end, they argue that a matrix of obligations could help states and stakeholders to demonstrate compliance with cyber norms and international law and, if risk assessments and prioritizations were done, could help guide action plans for implementation.

In Chapter 4, Zhanna L. Malekos Smith examines what governance mechanisms and capacity building initiatives are functioning well in outer space and proceeds to make the case for how these measures might be applied towards promoting accountability in cyberspace. In exploring this question, Malekos Smith examines the Artemis Accords and capacity building mechanisms for the long-term sustainability of space activities. She further highlights the deepening relationship between outer space and cyberspace—an intersection which may require its own governance and accountability mechanisms, or better integration and application of existing norms and law for this new context.

In Chapter 5, Decker and Rauhut discuss the Montreal Protocol on Substances that Deplete the Ozone Layer. One of the lessons they draw from analyzing the Protocol is that different capacities lead to different risk appetites but that these differences can be balanced by incentive structures. This was a core aspect of the process leading to the adoption of the Protocol. In cyberspace this is also true—many countries value low-cost and potentially less secure ICT as possibly worth the gains from quicker and cheaper digitization. Professional panels provide assessments of technology and economic alternatives to help customize approaches for reducing risks within each country as part of reducing overall societal risks.

In Chapter 6, Rosa Celorio outlines the applicability of international human rights law and related peer review mechanisms to cyber and digital security. Celorio argues that there is scope to better integrate concerns about cyber security and cybercrime within existing human rights peer review mechanisms such as the Universal Periodic Review (UPR). Current initiatives like the UN Global Digital Compact can support the identification of the human rights that are at risk in these areas and outline responsibilities for state and nonstate actors. Celorio stresses that UN Charter- and treaty-based bodies can also make critical contributions in specifying and defining terminologies when addressing digital threats to human rights.

In Chapter 7, Reece Iriye looks at the European General Data Protection Regulation (GDPR). He underscores the importance of clear and precise yet adaptable terminology in regulation, as well as centralized and uniform enforcement processes with oversight measures for managing major policy violations. Iriye notes this uniform approach simplifies the regulatory landscape for companies operating...
in multiple countries. He argues that regional organizations can play a significant role in shaping global policies in the digital and cyber field particularly in areas where private actors frequently operate, and cross-border interactions regularly occur. Iriye also stresses a focus on regulation of activities and roles instead of items and technology and the importance of building in opportunities for review.

In Chapter 8, James Siebens and Anne-Marie Buzatu discuss the approaches to “co-regulation” of the private military and security industry undertaken by states and private companies through The Montreux Document on pertinent international legal obligations and good practices for states related to operations of private military and security companies (PMSCs) during armed conflict and the subsequent establishment of the International Code of Conduct for Private Security Service Providers. The authors argue that these examples may provide a useful model for how to establish common interpretations of how international law applies in cyberspace, as well as clarifying and fostering accountability around the legal obligations and normative commitments of both states and private companies engaged in relevant cyber activities.

In Chapter 9, Moliehi Makumane explains that the experience of the African Peer Review Mechanism has demonstrated that there is a will to participate in regional peer review processes. To integrate cyber security into regional mechanisms at scale, it will be crucial to establish a relationship between regional peer review mechanisms and UN cyber processes which should encourage states to be transparent on their activities in peer review self-assessments. As with any accountability measure, Makumane notes that a crucial key to success is ambition.

In Chapter 10, Debra Decker argues that market mechanisms such as insurance, credit ratings, product/service security ratings and liability adjustments, as well as tax adjustments and grants, are currently relatively untapped incentives that can play a pivotal role in promoting accountability for securing cyberspace. Of these, Decker explores the expanding interest in the role of the insurance industry in driving and defining accountability.

Finally, in Chapter 11, Allison Pytlak and Shreya Lad examine activities and initiatives being implemented by the International Telecommunications Union (ITU) and argue that these could be better leveraged in the pursuit of cyber accountability. This includes the Global Cybersecurity Index, establishment of national cyber security strategies, and activities that support National Computer Incident Response Team (CIRTs) in helping states, assess threats, build resilience, and promote accountability.

The above contributors were invited to analyze these specific issue areas to assess the potential relevance to cyber accountability, and the legal, normative, or informal and market-based mechanisms that were developed to address accountability gaps therein. While the topics of the case studies are quite diverse, each addressed consistent research questions: how was the mechanism developed; how it is intended to function; any enforcement mechanisms; and the degree to which they have been effective in structuring incentives and shaping behavior in each issue area. The experts also offer views on how the mechanism under question is relevant to cyber. In some instances, there is a direct relationship while in others it is more about lessons learned that are instructive for a particular cyber governance challenge.

Some experts offer reflections about gender dynamics within the negotiation of these instruments, or about how gender equality and gender-responsiveness are relevant.
This collective analysis has produced a diverse toolkit of accountability models and mechanisms, ranging from legally binding treaties to regional-level peer review processes to insurance standards. Based on these structured analyses, contributors each proposed a set of recommendations linking the case studies to emerging cyber issues, or identifying the unique benefits, successes, and failures of the mechanisms they studied in order to inform similar efforts in cyberspace.

In some areas, we identified specific accountability mechanisms and tools such as institutions, agreements, or reporting instruments that were selected to examine further for their applicability to cyberspace. In other areas the initial research revealed relevant and cross-cutting lessons about the role of nongovernmental stakeholders, including proxy and mercenary actors, or transparency and incentive structures that may be adapted to suit specific challenges in the cyber domain, or which may already be suited to addressing or mitigating cyber threats and risks by direct application.

The research and our collective findings are largely predicated on global frameworks and cybersecurity and cybercrime efforts such as existing international law, the UN Framework, the UN Cybercrime Treaty process, and multilateral initiatives such as the Counter Ransomware Initiative and the Pall Mall Process, among others.

In addition to this case study research, this report has benefitted from input and experts from civil society, private industry, and governments during a series of workshops held under the Chatham House Rule. Workshop participants discussed the concept of accountability and how it might be applied to malicious activity in cyberspace. They also provided advice on the research design during early stages of the project, and later offered feedback and constructive critiques on the preliminary results of the case studies as well as the report findings and recommendations.

With EU Cyber Direct, the Stimson Center has co-published five briefing papers that examine various dimensions of cyber accountability as a complement to this report. Topics include the relationship to deterrence, capacity building, and regional perspectives from Africa, Europe, and Latin America.

Importantly, this report does not seek to identify or recommend one particular pathway or model as the best option to creating accountability for, or deterring, malicious activities in cyberspace. Instead, the report is designed to set out a range of policy approaches and considerations for policymakers, considering both the analyses of the case study authors and the input collected during multistakeholder expert workshops. As such, the report seeks to identify accountability mechanisms with the greatest potential value and relevance to addressing cyber gaps and challenges, while deliberately leaving the assessment of which approaches are most feasible or desirable to those responsible for preserving international peace and security.
Endnotes

1 Antonio Guterres, A New Agenda for Peace, Policy Brief 9, United Nations, July 2023, p.27.

2 Why the emphasis on accountability? According to James A. Lewis, a senior researcher with the Center for Strategic and International Studies, an effective international cyber strategy must focus upon the following three elements: “how to build resilience, to create a collaborative defense, and how to produce accountability in cyberspace (and this should include a discussion of when and how to disrupt opponent operations).” James Andrew Lewis, “Deterrence and Cyber Strategy,” Center for Strategic and International Studies, November 15, 2023, https://www.csis.org/analysis/deterrence-and-cyber-strategy.

3 See, for example: Jason Healey, Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies, February 23, 2022; and Patryk Pawlak, Accountability in Cyberspace: The Holy Grail of Cyber Stability?, EU Cyber Direct, March 2024. Relevant research and events have also been produced by The Hague Program on International Cyber Security at Leiden University, the EU Institute for Security Studies’ EU Cyber Direct Program, and the Royal United Services Institute’s project on Responsible Cyber Behavior.


5 UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, July 23, 2015. Eight norms are actions that states want to encourage, while the other three involve actions that countries should avoid. The framework is primarily about promoting interstate cooperation, respecting human rights and privacy, protecting critical infrastructure, safeguarding global supply chains, providing assistance when required and preventing the malicious use of digital technologies on states’ national territories. See https://www.aspi.org.au/cybernorms for more detail.


2. Reimagining Cyber Arms Control

Allison Pytlak

Introduction

A healthy debate has existed amongst academics and policymakers for more than a decade on the feasibility of applying traditional arms control and nonproliferation approaches to international cyber security. Some experts posit that there are too many differences for these fields to have any relevance, whereas others have identified specific experiences, principles or frameworks which they view as instructive or even directly applicable for addressing diverse cyber threats. From an accountability perspective, the broad success of many arms control and nonproliferation mechanisms and tools for improving transparency and enhancing cooperation makes them appealing and of interest—whether as a model for possible new instruments in cyber or as mechanisms that might be updated to account for digital technologies.

This chapter presents a simplified overview of the main arguments for and against an arms control approach to international cyber security. This is followed by case studies examining two arms control mechanisms—the Arms Trade Treaty (ATT) and the Wassenaar Arrangement—from which we identify relevant take-aways for cyber.¹

Cyber, Arms Control, and Nonproliferation

Arms control is traditionally understood as efforts that seek to restrict or control the development, production, stockpiling, proliferation and usage of arms including small arms and light weapons (SALW), dual-use items², and weapons of mass destruction (nuclear, chemical, and biological).³ Arms control often includes measures that seek to increase the transparency of military capabilities and activities, with the intention of reducing the risk of misinterpretation or improving trust and confidence.

Nonproliferation is an aspect of broader arms control efforts. Nonproliferation refers to activities that seek to prevent the spread of weapons and capabilities to new actors. As observed by one group of scholars, “The purpose of nonproliferation regimes includes: minimizing instability; increasing predictability in relations between potentially hostile states; pre-empting the development of new weapons; contributing to conflict management by establishing a framework to enable negotiations among parties, generally fostering a non-hostile atmosphere.”⁴

It is important to underscore that arms control and nonproliferation efforts are regimes composed of formal and informal mechanisms, including legally binding agreements as well as informal trust-building
measures and information-sharing, among other activities and agreements. Arms control is “not simply about legally binding, verifiable treaties between states, although these are of course welcome, but rather all measures designed to dampen incentives to begin hostilities, limit the damage if conflict should occur, and that enhance stability.”

Critics of applying arms control and nonproliferation approaches to cyber security offer a range of arguments and perspectives. Many of these tend to coalesce around some common and often interrelated points, as summarized non-exhaustively below.

**DEFINITIONAL CHALLENGES**

Arms control and nonproliferation are precise and specific in the items they apply to, even those that are dual use. A primary challenge for cyber arms control or nonproliferation efforts has always been the question of what is being controlled. Various efforts to define a “cyber weapon” have been made, but they lack universality. Diverse experts further note that the inherently dual-use nature of ICT tools and what some consider to be “cyber weapon” is different than how dual-use has been understood and applied within traditional arms control. Others have noted that the subcomponents of a “cyber weapon” could be subject to different legal regulation based on their nature (i.e. some may be dual-use, others inherently military in nature).

As such, defining cyber weapons is not straightforward “as many weapons of cyber nature may not be weapons unless used in a specific way”. Others have noted the challenges inherent in tracking and controlling items that are virtual, which cannot be destroyed but can be regenerated, or which may not also have universal lethality. Some stress the role that purpose and intention play when trying to determine if an item or tool could be deemed a cyber weapon.

**VERIFICATION**

Virtually all commentaries on cyber arms control and/or nonproliferation highlight the central challenge of verification, and relatedly, compliance and enforcement. One source summarizes the cyber verification problem as having “two prongs”. The first is about being able to ascertain the size of a state’s cyber arsenal, per the definitional challenges already described, and the second prong relates to monitoring efforts to ensure future compliance.” This second prong is made complicated given that the covert nature of cyber operations generates reluctance among governments to agree to verification methods that “…could expose a state’s own cyber capabilities, but also reveal gaps in its defense.”

Some have identified methods that would serve verification purposes in ways that are mindful of the unique contours of cyber security. While it has not gained widespread political traction, a variety of nongovernmental stakeholders have in recent years explored the possibility of developing a Global Cyber Attribution Consortium composed of nongovernmental experts utilizing a transparent and standardized approach to attribution for cyber operations.
COMPLIANCE, ENFORCEMENT, AND ATTRIBUTION

Following on from the above challenges of verification, there are issues relating to compliance and enforcement of any cyber arms control or nonproliferation agreements, and by extension—attribute, whether technical, legal, or political. As one group of scholars has explained, “Primarily, cyberattacks can be carried out in relative anonymity. The peculiarity of secrecy and plausible deniability of the attack makes it very hard to sanction the states from which the attack has been carried out. Therefore, any constraint in the use of cyber weapons would at least require a solution to the attribution problem. Moreover, malicious software is abundant and extremely difficult to identify and suppress. Therefore, an international agreement on cyber arms control would currently face serious problems with verification and enforcement.”16

OTHER FACTORS

The literature also variously touches on other factors, including the diversity of actors in cyber and their respectively varied levels of authority;17 the rate of technological change and progress; the necessity of political will; and the emphasis placed by some experts on the complementary yet unique role of deterrence, however it is defined or understood in a cyber context.18

There are also arguments pointing to the utility of applying arms control and/or nonproliferation approaches to the cyber domain. Yet, most proponents are quick to stress that the concepts and agreements themselves cannot be transferred to the cyber domain wholesale. Rather, one could look to particular concepts or frameworks that are instructive or that there is value in studying the policy and diplomatic processes leading to the negotiation and adoption of various mechanisms, not least given the politically challenging contexts in which many such mechanisms were forged.19

For example, the potential value of no-first-use policies, de-targeting, confidence building, prohibition on the development of certain hazardous technologies, cooperation for peaceful purposes, and regional arrangements have been examined as particularly salient concepts.20 Several scholars have stressed the potential of confidence-building measures (CBMs), which already exist within certain regions and sub-regions for cyber security purposes.21 Other relevant experiences from small arms control instruments include learning from national reporting practices, the involvement of civil society and other stakeholders, and the role that different types of instruments and mechanisms can play in achieving particular cyber stability goals.22 Demilitarized zones are an important aspect of some arms control agreements; it could be worth interrogating whether it is possible to define similar zones or perimeters for cyber, that should be excluded from warfare.23

It has been stressed that any form of cyber arms control will likely involve a mixture of formal and informal mechanisms and intermediary steps, and be single-issue and focused rather than broad and general.24 Cyber arms control could also be approached from a preventive or regulatory perspective.25 In this vein, some scholars have encouraged an approach that seeks to regulate behaviors and outcomes rather than the technologies themselves which could help to overcome challenges relating to definitions, dual-use, and ongoing technological development.26
Case Study 1: The Arms Trade Treaty

The international Arms Trade Treaty (ATT) is a legally binding arms control treaty adopted by the UN General Assembly (UNGA) in 2013 and entered into force in 2014. It is often considered groundbreaking because of the extent to which human rights and humanitarian concerns are integrated into the obligations of State parties have with regards to controlling the transfer of weapons.

The ATT seeks to regulate the international trade in conventional arms by establishing the highest possible common international standards for doing so and thereby seeking to prevent and eradicate the illicit trade and diversion of conventional arms. The Treaty’s text sets out the scope of weapons and items it applies to, as well as obligations for exporters, importers, and transit states. It also contributes to transparency and information exchange through its provisions on reporting.

As of early 2024, the ATT has 113 State parties and 28 signatories (countries that have signed but not yet ratified it) including Singapore and the United States; the latter of which “unsigned” the treaty in 2019. Fifty-four countries remain outside the ATT, including India, Pakistan, Russia, and Saudi Arabia.

A core component of the ATT is its risk assessment procedure and related criteria as set out in Articles 6 and 7. Under Article 6, all State parties must consider the potential impact of each arms transfer against specific criteria, such as the existence of an arms embargoes or the likelihood that the arms in question would be used in the commission of genocide, crimes against humanity, grave breaches of the Geneva Conventions of 1949, attacks directed against civilian objects or civilians, or other war crimes as defined in international agreements to which it is a Party. Transfers that would contravene the above are prohibited.

Article 7 offers a “second step” of the risk assessment process for items that are not stopped by the considerations of Article 6. Here, the exporting state must consider if the export in question could be used to commit or facilitate a serious violation of international humanitarian law or of international human rights law; or commit or facilitate an act constituting an offence under international conventions or protocols relating to terrorism or transnational organized crime. Notably, there is also a requirement to consider the risk of the arms being used to commit or facilitate serious acts of gender-based violence or serious acts of violence against women and children.

Other parts of the Treaty set out guidelines for states that are importing weapons and require importers and exporters to cooperate in sharing information necessary to make the above assessment. It also includes obligations for countries that have weapons transiting through their borders and for brokering activities. Article 11 is devoted to provisions and actions that address concerns around the diversion of arms transfers to illicit markets.
States must conduct a risk assessment before they say yes or no to an arms transfer:

- Will it contribute to or undermine peace and security?
- Could it be used to commit... violations of human rights law?
- Could it be used to commit... violations of humanitarian law?
- Could it be used to commit... organised crime?
- Could it be used to commit... gender-based violence?
- Could it be used to commit... terrorism?

If risk is too high, state shall not authorise the transfer.

Article 7 of The Arms Trade Treaty requires states to conduct risk assessments before authorizing exports of regulated arms.

Image by the Control Arms Coalition.

IMPLEMENTATION AND ENFORCEMENT

The ATT contains no explicit enforcement mechanism. Article 14 (on Enforcement) outlines that “Each State Party shall take appropriate measures to enforce national laws and regulations that implement the provisions of this Treaty.”

The Treaty does, however, have requirements for national reporting, found in Article 13. State parties are obligated to submit two reports: an Initial Report shortly after joining the Treaty, and an Annual Report. The Initial Report helps to provide a snapshot of a state’s arms control policies and practice upon joining the Treaty, whereas the Annual Report includes information “concerning authorized or actual exports and imports of conventional arms covered under Article 2(1) that were made during the preceding calendar year.”
Overtime, voluntary templates have been developed for both and reports and are made publicly available—unless otherwise indicated—on the ATT website. Since 2013, the Arms Trade Treaty Baseline Assessment Project (ATT-BAP) at the Stimson Center has supported states in understanding the obligations of the ATT and to promote effective implementation. ATT-BAP has developed tools to help provide a baseline for assessing progress in implementing the ATT and to enable measurement of the treaty’s impact and long-term effectiveness. These tools are also utilized for identifying state capacity and resource needs, including the identification of critical gaps and available resources to implement the ATT.

State parties meet annually for a Conference of States Parties (CSP), and there are often two “preparatory committee” sessions, or PrepComs, held during the intersessional period to prepare for the CSPs. Over time, ATT State parties have established three permanent working groups: on Treaty Universalization; Effective Treaty Implementation; and Transparency and Reporting. Some of these have established further sub-working groups or subsidiary bodies. The Groups meet during the PrepComs and tend to be where more focused documentation or outputs are developed and later tabled for possible endorsement at CSPs.

Over the years the Working Groups have, in this way, been able to produce extensive resources to support the ATT including toolkits and guidelines relating to Treaty interpretation or implementation, incentivizing Treaty universalization, or to aid in meeting reporting requirements. Working Groups are open to the participation of any state as well as nongovernmental organizations and have different approaches for selecting chairpersons to lead their work.

The ATT has a small Secretariat in Geneva, and the Treaty presidency rotates annually. Financial contributions are based on the UN Scale of Assessments and are used to support CSPs and other meetings and core Secretariat functions.

**HOW WAS THE ATT DEVELOPED?**

The ATT is the product of over a decade of committed advocacy and diplomacy. The idea began with Nobel Peace Laureates, supported by civil society organizations worldwide who were concerned about the unrestricted spread of weapons following the end of the Cold War and their role in fueling conflict, poverty, and human rights abuses. With its focus on the legal trade in conventional weapons, the proposed ATT was a complement to earlier instruments that targeted illicit trafficking in conventional arms, notably the 2001 UN Programme of Action on small arms and light weapons.

A 2006 civil society-led “Million Faces” petition contributed to the start of a diplomatic process inside the United Nations (UN). In 2009, the UNGA launched a time frame for the negotiation of the ATT. This included one preparatory meeting in 2010, two in 2011, and a negotiating conference in 2012.

The four-week long negotiating conference produced a draft treaty text but failed to adopt a treaty by consensus after the United States, Russia, and a few other states blocked adoption. A mandate was obtained via the UNGA to hold a Final Conference in March 2013.

Negotiations continued over particular provisions and treaty language, some of which generated so-called “loopholes” in the treaty’s text. Unfortunately, consensus was also blocked in the final hours of the Final Conference. Many member states from diverse global regions moved to take the draft treaty to
the General Assembly to be adopted by a vote. This vote occurred on 2 April 2013, when the Treaty was finally adopted by a vote of 154 in favor, 3 against, and 23 abstentions.

As with any multilateral instrument, the negotiations were complex and hard-fought; certain proposals that may have enjoyed high levels of support at one stage of the process were lost or modified along the way. Any legal mechanism or framework is ultimately a product of compromise and lands where negotiators can find sufficient middle ground.

As noted above, the role of nongovernmental stakeholders throughout the treaty process was significant. While many of these groups came from civil society, including survivors of armed violence, arms industry representatives and investors also attended or contributed to the treaty's development. It is also noteworthy that there was strong opposition to the ATT from pro-gun groups in the United States, who tried to frame the agreement as counter to U.S. gun ownership rights.

**IMPACT AND EFFECTIVENESS**

Views on the impact of the ATT and its implementation are mixed. In general, the overall record of implementation has been found to be lacking. Critics, mainly but not exclusively from civil society, have pointed out that some State parties continue to transfer arms to recipients that are likely to use them in violations of human rights and IHL, or that it has served to facilitate the trade in arms rather than prevent harmful transfers and that there are no consequences for perceived violations.

Russia and other major exporters remain outside the Treaty. The United States signed but did not ratify the ATT; former President Trump tried to “un-sign” the U.S. from the agreement in 2019.

Like many other multilateral arms control and disarmament instruments, the ATT is experiencing financial challenges due to membership dues that are in arrears. Concerns have also been raised about the status of Treaty reporting, which has declined in recent years, and about more State parties choosing to keep their reports private.

Positively, the Treaty enshrines in international law the relationship between human rights and the negative impact that international arms flows can have. In particular, its provision on gender-based violence (GBV) is considered groundbreaking as it requires State parties to consider the probability of the arms in question being used to commit or facilitate GBV, or serious acts of violence against women and children.

The ATT has also created a single standard of practice for the international community. Prior to the ATT, arms export (and import) policies were governed by a patchwork of unilateral, bilateral, and regional agreements and policies; this created legal loopholes that facilitated illicit arms trading and diversion to illicit markets. While the ATT is not yet fully universal, high levels of cross-regional membership have helped to “level the playing field” and set more common policies and practice, which in turn have closed some of the pre-existing loopholes and grey areas that existed as a result of the patchwork approach to regulation.

The Treaty’s implementation has also fostered a community of experts from within and outside governments who convene regularly to discuss and assess issues of international arms trading. The volume of toolkits, guidelines, model legislation, workshops and other resources that have been produced since
the Treaty’s entry into force is not insignificant and has gone a long way to foster greater cooperation and understanding about international arms flows and has contributed to national-level measures such as the establishment of control lists, policies, and more.

A voluntary trust fund mandated by the Treaty support countries with treaty implementation. It has supported 83 projects since 2016. Implementation assistance covers a range of activities from procurement and training in firearms marking, to helping develop legislation or national control lists. The ATT International Assistance Database is a secure web-based platform that enables states to submit requests and offers for assistance for Treaty implementation on a voluntary basis.

**RELEVANCE TO CYBER**

Recognizing that the ATT is a legally binding instrument—an unlikely scenario in the cyber context at present—it nonetheless offers experiences and practice that can be instructive for advancing cyber accountability.

The negative impact of some cyber and digital tools on human rights is increasingly well-documented and attracting attention from policymakers. As such the experience of the international community, working together with legal, technical and subject matter experts to develop common criteria for the Treaty’s risk assessment process rooted in human rights and IHL is instructive for efforts to limit cyber surveillance or intrusion software, or to regulate the activities of those who produce and distribute such items. This may also be instructive for parsing out differences between irresponsible, illegitimate, and illegal. The central role of human rights, international human rights law (IHRL), and international humanitarian law (IHL) is deeply relevant for those who want to see more rigorous application of relevant cyber norms and legal principles within the cyber security field and demonstrates that international security and human rights considerations can be integrated within policy frameworks.

The ATT is also important for harmonizing what had previously been a patchwork-style approach to international arms transfers, comprised of various regional treaties and differing national practice. This is similar to the function that UN Security Council resolution 1540 played for dual-use items that can be used for the production, development, or delivery of weapons of mass destruction. Patchwork approaches sometimes inadvertently create loopholes or incompatibilities between instruments, which become exploitable. This makes it important to harmonize and clarify obligations and responsibilities. That said, there is always a risk that “leveling the playing field” will water down high standards to a lower common denominator.

While the ATT does include a scope of physical items that the treaty applies to, it also has a heavy focus on regulating behavior and activities, and the role of diverse non-state actors including brokers, those engaged in transit and transshipment activities, among others. A focus on behavior rather than on items or “cyber weapons” is a recommendation that has come through from diverse cyber arms control experts, as outlined in the introduction. Even then, more clarity would be needed as to what constitutes a cyber weapon in order to introduce controls: capacities for offensive cyber warfare (computer network attacks), espionage operations (computer network exploitations), information operations, or the use of cyber technologies that are primarily a threat to human rights?

Finally, on a functional level, there are also lessons to be drawn from activities relating the ATT approach to working groups and reporting initiatives. The working group format, which is open to nongovernmental
stakeholders may be particularly useful for the UN OEWG or a future Cyber Programme of Action. Likewise, the experience of reporting templates and in particular Stimson’s contribution through the Baseline Assessment Survey are instructive for UN-based activities such as surveys of national implementation or interest in monitoring norms operationalization.

Case Study 2: The Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, or Wassenaar Arrangement (WA), is a voluntary export regime established in July 1996. It is the successor to the Coordinating Committee for Multilateral Export Controls (COCOM), which was created to restrict exports of conventional arms to the former Soviet Union and Eastern bloc.

According to its founding document, the WA was:

...established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals and are not diverted to support such capabilities.

The founding document also stresses that the WA seeks to complement and reinforce the export control regimes for weapons of mass destruction and their delivery systems; is not directed against any state or group of states; and uses export controls to combat terrorism.

Participation in WA requires that states be producers and exporters and must implement national export control laws that prohibit the sale of arms or sensitive dual-use goods to areas of concern. In line with its mandate, Wassenaar Members are expected to behave in accordance with international nonproliferation norms and standards such as the Nuclear Nonproliferation Treaty (NPT), the Missile Technology Control Regime (MTCR), the Chemical Weapons Convention (CWC), and the UN Register of Conventional Arms. There are presently 42 Participating States, 33 of which are founding members.

HOW DOES IT WORK?

The WA is comprised of two types of control lists: a munitions list for conventional weapons; and a list of Dual-Use Goods and Technologies. This second list is further divided into nine categories as well as a “Sensitive List” and “Very Sensitive” list. The WA operates via agreement among Participating States that they will control exports and retransfers of items contained on these lists, through national legislation which is guided by agreed Best Practices, Guidelines or Elements. Members also agree to report on transfers and denials of specified controlled items to destinations outside of the Arrangement, and to exchange information about sensitive dual-use goods and technologies.

The Arrangement does not prohibit a participating country from making an export to a particular destination that has been denied by another participant, but participants are required to notify other
participants within 60 days, and preferably within 30 days, after they approve a license for an export of sensitive dual-use goods that are essentially identical to those that have been denied by another participant during the previous three years. This has the potential to aid in accountability by improving transparency, provided that states follow through on the requirement.

Representatives of Participating States meet regularly in Vienna, which is where the headquarters and secretariat are based. The Plenary is the decision-making body of the Arrangement, composed of representatives of all Participating States and meets annually. The Plenary Chair position is subject to annual rotation and all decisions are taken by consensus. Subsidiary bodies are established for the preparation of recommendations for Plenary decisions and calls ad hoc meetings for consultations on issues related to the functioning of the Wassenaar Arrangement. Participating States also identify “Vienna Points of Contact (VPOC)” who are called for periodic meetings by the Plenary Chair to facilitate intersessional information flow and communications between and among Participating States and the Secretariat.

The Arrangement does not contain any specific enforcement mechanisms, in that Participating States do not have access to tools by which they can compel their peers to conform to export control arrangements.

**HISTORICAL DEVELOPMENT**

The establishment of the WA is closely interwoven with modern political history and geopolitics, specifically the end of the Cold War. The WA’s evolution, notably in relation to decisions and procedures around membership, scope, and enforcement likewise affects dynamics and tensions amongst members in the present day.

For four decades, the primary international organization for coordinating restrictions on dual-use exports among western states was the Coordinating Committee For Multilateral Export Controls (COCOM) which was first established in 1949. The focus of COCOM was to control exports to the Soviet Union, Warsaw Pact states, and from 1957 onwards, China. COCOM’s membership included 17 countries, including all members of NATO (except Iceland), Japan and Australia. Notably, it operated on the basis of consensus (interpreted as unanimity) and functioned without any legal basis or authorization. The practice of consensus effectively gave any Participating State a veto over the export of a controlled good or technology by any other Participating State to the Soviet Union, a Warsaw Pact state or after 1957, China. COCOM was disbanded in 1993 and its members agreed to replace it with a new entity and move to a model of “national discretion” in arms export control, in which no state could veto the export decisions of another. Efforts to create a replacement entity was driven largely by the United States in the context of its other efforts at the time around promoting policies of “multilateral restraint” in the area of arms exports. The newly established WA had a wider and more heterogenous membership than COCOM had and was also different in not naming explicit targets and in including conventional weapons. The emphasis on “national discretion” meant that there is not a centralized body or entity responsible for overseeing if Participating States are acting in conformity with the WA or playing a role in deciding about arms transfers. In 2000, the plenary adopted a set of Best Practices for effective enforcement, in the areas of preventive measures, investigations, effective penalties, and information exchange.
IMPACT AND EFFECTIVENESS

There are different views on the impact and effectiveness of the Wassenaar Arrangement. Many see its value as a cornerstone of the modern arms export control regime, in which context it has facilitated or enabled the development of other agreements and frameworks, or aided with confidence-building, information exchange and transparency efforts.

Yet the potential benefits are undermined by the limitations of its membership, in that non-Participating States do not have access to reports. The absence of significant arms exporters such as China and Israel has also been cited as a limitation\(^54\) although Israel has put in place legislation which adopts all Wassenaar controls automatically.\(^55\)

Membership has had implications for other aspects of the WA's implementation. While broader than COCOM, most members are Western developed countries, causing some non-Western states to view the WA negatively, and as an exclusive club or as an extension of Western (notably US) approaches and practices to arms export control.\(^56\) Yet even amongst the membership there are different views on core issues such as the instrument's scope or about which recipient countries can be deemed “states of concern”. For example, the United States has sought to target particular countries, such as Iran, Iraq, Libya, and North Korea, but others have supported the Wassenaar Arrangement’s “impartiality” on this issue.\(^57\) As currently constructed, Wassenaar “will not, however, be directed against any state or group of states; impede bona fide civil transactions; nor interfere with the rights of states to acquire legitimate means with which to defend themselves.”\(^58\)

Russian membership has been controversial and has many implications for consensus-based decision making within the WA, as in all other multilateral fora. Some note that Russian participation has allowed the international community to have some transparency on Russian export activity, but there has not been a corresponding change in decision-making as concerns Russian approval of exports to unstable regions. Since 2022, the issue of Russia blocking proposals for new control list items has become more of an issue. The U.S. stated that Russia had blocked proposals relating to the controls of quantum technologies and the Netherlands reportedly held back on a proposal for new controls of semi-conductor manufacturing equipment given the low likelihood of consensus in the WA right now.\(^59\)

One empirical study of arms import data has shown that the WA has had a limited impact on preventing “destabilizing accumulations” of conventional weapons and no clear evidence of a shift in arms trade because of the regime’s formation.\(^60\) Unlike the ATT, decisions about export control under WA do not consider potential human rights violations; national security considerations form the basis.

Relevance to Cyber

In recent years, the WA has adapted to technological change by expanding the scope of its control lists in ways that have drawn attention to the instrument from within the cyber community. Some trace this back to initiatives within the WA undertaken during the late 1990s and early 2000s in relation to adding encryption techniques and technologies.\(^61\) This prompted the international cyber security community to increasingly focused on the WA’s potential application to dual-use information and communication technology, perhaps more than other arms export control mechanisms. As such, the
ability of the WA to foster greater accountability or transparency within the cyber domain is already being evaluated in real-time.

The way in which the early efforts on expanding the WA to include encryption unfolded influenced how the technology sector would view later efforts concerning other technologies and the move to a “cyber arms control” approach. It also ushered in an era of greater involvement within the work of the WA from nongovernmental stakeholders including cyber security professionals, lawyers, academics and activists.

In 2010, revelations about the use of digital surveillance technologies by oppressive governments prompted the EU and U.S. to consider steps that would seek to restrict their proliferation. Several of the firms producing such technologies were based in European countries, and had been exporting their products to, among other clients, governments with poor human rights records; in some instances, such products were directly linked to the repression of journalists and activists.

In 2013, France and the United Kingdom took initiative to introduce the first significant amendment to the WA to adopt a set of controls that would cover certain surveillance and intrusion tools, notably IP surveillance systems and intrusion software. As described in the 2013 plenary statement:

New export controls were agreed in a number of areas including surveillance and law enforcement/intelligence gathering tools and Internet Protocol (IP) network surveillance systems or equipment, which, under certain conditions, may be detrimental to international and regional security and stability. Participating States also further clarified existing controls in respect of inertial measurement equipment or systems and relaxed some controls such as for instrumentation tape recorders and digital computers.

IP surveillance systems were added to the part of the Dual-use List that covers the category of “Telecommunications” in a way that set out various conditions in order to determine if the different aspects of a system in question fall under the control list. Intrusion software was included within the “Computers” section of the Dual-Use List. The provision covered components used to generate, install, or control intrusion software—rather than intrusion software itself—in an effort to target the producers rather than targeted individuals who may end up with the components on their devices. As a result of these and other related changes to WA, companies developing and selling these types of tools from within Wassenaar countries must now apply for a license from their governments before exporting their products abroad.

In 2015, U.S. efforts to implement the 2013 amendment nationally caught the attention of cyber security professionals. Cyber companies and other civil society actors have raised a variety of concerns over the amendment’s content, as well as about ensuing actions taken within the United States domestically and later developments in the Wassenaar Arrangement. In brief, one big concern was that the definition of the software being controlled was overly broad and vague, and thus would potentially encompass many legitimate security tools, such as those used for penetration-testing and some security research. There was some pushback on exemptions to penetration testing tools within software controls. Vulnerability disclosures were also a concern because the U.S. indicated it might use intrusion software controls to regulate the trade in zero days. The implications of this for other states, as well as for international collaboration of identifying and reporting vulnerabilities.
Some of these controversies were due to insufficient engagement with technical experts—notably security researchers—and potentially due to confusion or lack of adequate communication and coordination between the different U.S. government departments involved in international talks versus those tasked with implementing the WA decision domestically.

The concern over what technologies would be subject to export controls united a diverse set of nongovernmental cyber security experts and practitioners, ranging from human rights groups to tech companies and security researchers, in an effort to motivate the U.S. government to push for changes within the WA. This was accomplished in 2016 and 2017 via a series of exemptions that are based on the intent of the user (i.e., for vulnerability disclosures and cyber incident response) and work to clarify definitions and understandings around terminology.\(^9\)

In early 2024, Switzerland proposed controls on another cyber-surveillance tool in the Wassenaar list but, experts feel it is not certain to be adopted given the divisions among members described earlier.\(^7\)

Ongoing activity within the WA make it somewhat challenging to evaluate the instrument for lessons learned for cyber accountability on its own merit as an export control instrument and not in relation to cyber and ICT-related debates within WA. Moreover, export control is not universally viewed as the best vehicle for slowing the spread of ‘cyber weapons’ or continuous technological development, given the numerous ways that these ‘items’ can be exchanged and in ways far more challenging to track than conventional weapons.

That said, the experience of trying to update an arms export control instrument for a digital context provides important insights and observations that are relevant both for efforts within the WA as well as for the pursuit of other export-based avenues and frameworks, should they emerge. Calls to curtail the sale and transfer of commercial spyware and, relatedly, cyber mercenaries (understood here as firms developing and selling such spyware) are growing in urgency.

This might be an instance where leveraging the WA to enhance cyber accountability is a road to keep traveling down, but bearing in mind the lessons learned from past efforts. It helps bring into focus the importance of determining whether to attempt to control an item or a technology, or rather to set controls for state behavior and decision-making processes. Within that, the question of intent becomes critical.\(^7\) The practice of agreeing to report on transfers and denials of specified controlled items and to exchange information about sensitive dual-use goods and technologies is a boost to transparency and accountability, even it occurs within the non-universal confines of WA membership. Continuing to discuss and debate how to develop export control models for cyber and digital tools does have merit, as it helps to unpack and examine fundamental aspects of the cyber environment, and coordination amongst actors therein.\(^7\)

There are also lessons to be taken about the importance of engaging with nongovernmental stakeholders and experts and about the diverse ways in which international policy making can impact national policies and practice.
Key Takeaways and Recommendations

Building on both case studies and broader literature review of cyber arms control, we offer the following takeaways and recommendations for applying an arms control and nonproliferation approach to cyber:

1. **An approach which seeks to regulate behaviors and outcomes rather than technologies is more likely to overcome challenges relating to shifting definitions and ongoing technological development.**

   Additionally, and in the context of export control, updating and adapting the concept of “dual use” for digital technologies to make the term applicable to a broader scope of items is worth exploring. As some research notes, it would be more relevant and effective to approach duality from a starting point which acknowledges that many technologies are used in peacetime rather than in conflict and thus generate human rights concerns that have historically been beyond the purview of the dual use dichotomy.

2. **The toolbox approach of formal and informal mechanisms and mini regimes will enable policy and regulatory responses that are more focused on specific cyber threats and challenges than pursuing a single umbrella-type agreement.**

   As demonstrated by arms control and nonproliferation, there are a range of tools and mechanisms that can co-exist alongside formal mechanisms, including reporting, best practice exchanges, the production of guidelines, establishing working groups within broader forums, and confidence and trust-building measures. The toolbox might also include criminal law standards leading to prohibitive punishment. Yet, and as demonstrated by the case studies, a lack of compliance incentives will be problematic and reduce effectiveness of any instrument or tool. To be meaningful and effective, cyber accountability mechanisms should consider how to incentivize compliance or participation.

3. **Robust involvement of a diversity of nongovernmental stakeholders is crucial for success.**

   While this is an already widely known truth for many in cyber diplomacy or policymaking, there is also pushback and resistance to involving civil society or industry. The role of these and other types of stakeholders in the case studies presented here demonstrates the role these actors played in ensuring that the mechanisms in question aligned with real-world use of the items or technology in question or responded to real-world concerns. Yet, states must also be involved in, and assume their own responsibility for, malicious cyber activity.
Endnotes


2 Dual-use items that can be used both for civilian purposes and to produce, maintain or operate conventional, biological, chemical or nuclear weapons.


16 Barbieri et al., p.21.


Dahinden, “Can Arms Control and Disarmament contribute to a secure Cyberspace?”


Author’s email correspondence with a peer reviewer.

Futter, “What does cyber arms control look like?”

Meyer, “Cyber-Security Through Arms Control.”

Rheinhold, Pleil and Reuter, “Challenges for Cyber Arms Control.”

For more on the Arms Trade Treaty, visit https://thearmstradetreaty.org.


The tools include a Ratification Checklist, Implementation Checklist and Assistance Assessment, the ATT-BAP Baseline Assessment Survey, guidance for completing initial and annual reports, and numerous analytical reports.


The United States blacklisted NSO Group in 2021, a notorious producer of surveillance software, or spyware. Also in 2021, the European Union (EU) amended its regulatory framework on export control, the Dual-Use Regulation. The Regulation contains a new category, “cyber-surveillance items”, for which a new regulatory framework applies. In this new framework, human rights considerations play an important role. In 2023, the US released an executive order prohibiting the government from using commercial spyware that poses risks to national security. This issue is also being taken up through the Pall Mall Process, launched in early 2024.


Ruohonen and Kimppa.


Korzak, “Export Controls.”


An illustrative corollary comes from the Biological and Toxin Weapons Convention, which forbids research into the development of biological weapons but allows research for “protective purposes”. A program to develop a biological warfare agent is practically identical with research on protection yet the difference is the intention behind it, which cannot be verified by existing arms control verification instruments.

Herr and Rosenzweig, “Cyber Weapons and Export Control.”

Riecke, “Unmasking the term “dual use” in EU spyware export control.”
Advancing Accountability in Cyberspace, Stimson Center

The U.S. Army’s Weapons of Mass Destruction-Civil Support Team (WMD-CST) supports civil authorities at man-made or natural disasters by identifying chemical, biological, radiological, and nuclear substances. Image by Mark C. Olsen, New Jersey National Guard.
Introduction

United Nations Security Council Resolution (UNSCR) 1540 was adopted in 2004 in response to heightened global concerns about the dangers of weapons of mass destruction (WMD) and their potential impact on the international safety and security of the global commons. It provided an agreed framework for action to address WMD proliferation risks. Similarly, escalating security threats in the digital domain impact the global commons and have brought cybersecurity concerns to the forefront; a framework is needed for overseeing the implementation of agreed-upon cyber norms and laws.

The implementation of the 1540 resolution required states to adopt domestic laws and regulations to help ensure nonproliferation of WMDs and associated technologies. Several experts led in translating the resolution into a matrix for state implementation. This matrix has been instrumental in helping states to better understand their own responsibilities. In cyberspace, the UN has developed broad norms for responsible state behavior and affirmed the applicability of international law; however, what states and stakeholders need to do to evidence compliance with laws and norms has not yet been fully agreed upon.

The UN Security Council (UNSC) exercised its authority under Chapter VII of the UN Charter when it acted to protect international peace and security by unanimously adopting resolution 1540 in the year 2004. Resolution 1540 “imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and to establish appropriate domestic controls over related materials to prevent their illicit trafficking. It also encourages enhanced international cooperation in this regard.”

The resolution complements and strengthens existing mechanisms, informal and formal—including treaties for controlling nuclear, chemical, and biological weapons. It fills important gaps to complement other disarmament and nonproliferation frameworks. It takes a collaborative approach in that it does not require sanctions or other enforcement mechanisms. It does require states to implement domestic legislation to prevent proliferation including export controls and security measures for its materials and encourages accession to related international treaties.

UNSCR 1540 established a committee consisting of all UNSC members to oversee the resolution’s implementation with the assistance of what evolved into a Group of Experts (GOE). UNSCRs are binding on the entirety of the UN membership. Unlike the Committees of other subsidiary bodies to UN Security Council resolutions, the 1540 GOE has no agreed-upon mandate to engage with a UN member.
state without being prompted. The responsibilities of the expert group, as well as its independence, have been points of difference among some states.4

UNSCR 1540 resulted in part from post-9/11 concerns that nuclear, chemical, and biological weapons, as well as related materials and their means of delivery, could come into terrorists’ hands. While the United States (U.S.) had led development of the Proliferation Security Initiative (PSI) in 2003 to interdict suspected shipments of potential weapons of mass destruction and their means of delivery to terrorists and states of concern, it was a voluntary program with membership by invitation only and thus was not universally appreciated or adopted.5 In addition, the treaties controlling biological, chemical, and nuclear weapons were a patchwork with different memberships and provisions, creating an uneven global playing field.6

UNSCR 1540 was also driven by concerns about the privatization of proliferation that had emerged over the years leading up to 2004 resolution, in which nonstate actors including manufacturers, shippers, and brokers were increasingly providing WMD-related goods and knowledge to countries seeking WMD and/or their means of delivery. In February 2004 these concerns were heightened when Pakistani physicist A. Q. Khan gave a televised address in which he confessed to having a network for sales to support states’ nuclear programs.7

Early debates about UNSCR 1540 reflected some states’ concerns that the UNSC was overstepping its mandate by requiring states to prevent proliferation to all nonstate actors—both proliferation networks and terrorists—under the Security Council’s Chapter VII authorities.8 To address these concerns, the resolution was ultimately updated to reference the importance of states working collaboratively through relevant regional and international organizations. While the 2004 resolution established the 1540 Committee and recognized the need for it to integrate other expertise, it was not until later resolutions that there were direct calls for experts to support the Committee’s work. These resolutions formalized a Group of Experts in 2011 to support the Committee.9 Internal Committee debates ensued as to the appropriate scope of all the GOE activities, from providing implementation support to states to monitoring versus evaluating implementation progress.

**Developing Review and Assessment Mechanisms for Accountability**

The 1540 Committee supports states by responding to requests for assistance. This support has included assisting states to develop voluntary national implementation plans, providing matchmaking needs and resources, and collaborating within regional and other training programs. Peer reviews have been undertaken when states request them, although they are not done as frequently as for other, more targeted, agreements, such as in nuclear security.10

Many have questioned the aspects of UNSCR 1540 that call for “appropriate” and “effective” laws and measures to prevent proliferation, because countries differ in what they consider to be “appropriate.” Yet it has been useful to share model laws and effective practices, leading to shared understanding of these terms. When updating the UNSCR 1540 mandate through a new resolution in 2011 (UNSCR 1977), the UNSC asked the 1540 Committee to, with GOE support, “consider developing a technical reference guide to help implementation, including civil society and the private sector, with, as appropriate, their State’s consent”; however, this objective was not achieved.11
UNSCR 1977 also promoted a trust fund managed by the UN Office of Disarmament Affairs (UNODA) intended to fund travel and other projects involving the GOE, often in collaboration with nongovernmental organizations (NGOs). As the 1540 Committee’s Secretariat, UNODA is able to provide an important coordination role and uses the trust fund to support awareness-raising workshops, meetings, 1540 National Points of Contact trainings, and other activities including those on regional levels to help states implement the resolution.\textsuperscript{12}

Since the Committee’s GOE has no mandate, it is not permitted to directly suggest how each member state might best implement the resolution when all its aspects are ostensibly given equal weight. This lack of guidance makes it difficult for states to identify their highest risks as no structured, systematic approach to risk assessments has been or can be developed by the Committee with regard to any of the resolution’s requirements. Prioritization ends up being a function of what a state cares about on the one hand, and where it might most easily obtain knowledge and available support on the other. A promising approach has been to provide assistance with clear developmental benefits while encouraging fulfillment of state obligations under 1540.
FACILITATING INCENTIVES FOR AND ENSURING IMPLEMENTATION

The 1540 Committee supports states by responding to requests for assistance. This support has included assisting states to develop voluntary national implementation plans, providing matchmaking needs and resources, and collaborating within regional and other training programs. Peer reviews have been undertaken when states request them, although they are not done as frequently as for other, more targeted, agreements, such as in nuclear security.

Many have questioned the aspects of UNSCR 1540 that call for “appropriate” and “effective” laws and measures to prevent proliferation, because countries differ in what they consider to be “appropriate.” Yet it has been useful to share model laws and effective practices, leading to shared understanding of these terms. When updating the UNSCR 1540 mandate through a new resolution in 2011 (UNSCR 1977), the UNSC asked the 1540 Committee to, with GOE support, “consider developing a technical reference guide to help implementation, including civil society and the private sector, with, as appropriate, their State’s consent”; however, this objective was not achieved.

UNSCR 1977 also promoted a trust fund managed by the UN Office of Disarmament Affairs (UNODA) intended to fund travel and other projects involving the GOE, often in collaboration with nongovernmental organizations (NGOs). As the 1540 Committee’s Secretariat, UNODA is able to provide an important coordination role and uses the trust fund to support awareness-raising workshops, meetings, 1540 National Points of Contact trainings, and other activities including those on regional levels to help states implement the resolution.

This table demonstrates the relationship between WMD security imperatives and development.¹³
Since the Committee’s GOE has no mandate, it is not permitted to directly suggest how each member state might best implement the resolution when all its aspects are ostensibly given equal weight. This lack of guidance makes it difficult for states to identify their highest risks as no structured, systematic approach to risk assessments has been or can be developed by the Committee with regard to any of the resolution’s requirements. Prioritization ends up being a function of what a state cares about on the one hand, and where it might most easily obtain knowledge and available support on the other. A promising approach has been to provide assistance with clear developmental benefits while encouraging fulfillment of state obligations under 1540.

Demonstrating the value proposition of UNSCR 1540—that it complements the requirements put in place by other treaties and benefits the immediate domestic priorities of states—remains important. UNODA and others have additionally emphasized the link between fulfilling UNSCR 1540 obligations and realizing some of the UN Sustainable Development Goals.

An important auxiliary benefit of UNSCR 1540 is the internal and interagency coordination that reporting generates. Officials from ministries of foreign affairs, trade, finance, or various other science, technology, and health-related organizations are responsible for implementing aspects of the resolution. Their involvement begets the need to report on all 1540-related functions, which facilitates better internal coordination. UNODA provides self-paced and instructor-led courses on UNSCR 1540 implementation, including development of National Action Plans for 1540 Implementation. Forty-seven states have submitted such plans.

Countries with lesser capacity are hard-pressed to prioritize legislation or reporting because of the many complex and overlapping requirements among treaty-based agreements, UN resolutions, and export control regimes. NGOs have played an important role in this regard by providing prioritization suggestions where neither the Committee nor any given international organization lacked the capacity. Nongovernmental organizations therefore complement the Committee’s call for states to report more frequently whether to the Committee or domestically to legislative bodies and/or to executive branches of government.

PROMOTING AWARENESS AND BEST PRACTICES

The original (2004) UNSCR 1540 resolution specifically calls upon states “To develop appropriate ways to work with and inform industry and the public regarding their obligations under the resolution.” UNSCR 2325 adopted in 2016 emphasized this point and additionally noted the importance of outreach to parliaments as they enact the legislation needed to implement the resolution. A diverse series of activities have helped to promote awareness of UNSCR 1540 and best practices in its implementation.

Informing industry: Germany has hosted an annual conference since 2011, which evolved into regional meetings starting in 2016 known as the Wiesbaden Process to engage industry and others to support 1540 implementation. Germany then initiated a cooperation with UNODA and held the Erlangen Conference in Nuremberg in 2023 to collaborate with regulators and academia. Recognizing new emerging threats, these players engaged in providing “user-friendly” guidance on the transfer of intangible technology and emphasized the need for classification systems.
Leveraging civil society to promote accountability: Civil society can provide innovative ways to promote and support UNSCR 1540 implementation. Support has included help with drafting model laws, matching States with needed resources, and promoting awareness among students and others in academia.  

Promoting good practices: International organizations such as the World Customs Organization work with states, industry, and others to train officials and organizations on good enforcement and compliance practices that include UNSCR 1540 and related obligations, including controls over technology. The UN’s hope was that UNSCR 1540 could help to standardize export controls, bringing more countries and better processes to the export control supplier regimes. However, many member states disagree with this objective and are instead inclined to adopt more streamlined control lists that are more representative of the industrial activities taking place in their countries. In addition, state control lists can evolve, reflecting differing views on technological, economic, and security interests. Supplier regime lists change more slowly due to the time it takes to publish updated controls and the growing inability of states to agree on which updates, if any, are appropriate for some of these regimes.

Some countries work bilaterally via mutual assistance agreements with binding obligations to collaborate on customs law enforcement. However, stopping the illicit spread of technology has been hard, with states often unable to manage processes to identify, predict, and coordinate controls even within their own governments.

ADAPTING TO CHANGE AND PROMOTING LEADERSHIP

One mechanism that has worked to avoid bottlenecks in the UNSC’s 1540 Committee has been to establish regional 1540 coordinators that work with UNODA. This approach prevents a UNSC country from being able to stymie agreement on such issues as benchmarking standards of performance. Updates to the matrix may be forthcoming to reflect the role of new technologies in proliferation.

Most recently, UNSCR 2663 (2021) updated aspects of the original resolution (1540) and extended the 1540 Committee’s mandate by 10 years, reflecting that long-term commitment encourages implementation. For example, the language in the original resolution simply recognized the importance of controlling proliferation financing, while later resolutions encouraged work with the Financial Action Task Force (FATF).

The 2663 resolution’s establishment of a committee to support implementation enabled Security Council countries to take part in various specific roles with concordant responsibilities. The Committee then set up four UNSC working groups: 1) monitoring and national implementation; 2) assistance; 3) cooperation with international, regional, and subregional organizations, including UN bodies; and 4) transparency and outreach. The leaders of these working groups thus take on added responsibilities for ensuring successful implementation as does the 1540 Committee chairperson.
Key Takeaways and Recommendations

1. Find and Mind the Gap

Just as states did not initially and fully appreciate the potentially catastrophic nature of WMD proliferation risks, many today do not understand the potential enormity of risks that cyber and other emerging technologies such as AI present. Building value propositions around security and accountability for implementation of norms and laws is important. States have such wide-ranging needs that capacity-building is necessary to foster development along with security.

Recommendation: The true value proposition in investments in compliance with cyber norms and international law has not yet been made clear, and common interest in global cybersecurity needs to be strengthened. Local interests will differ among countries but must take account of the knock-on global effects that local decisions can have for issues like cyber and malicious ICT activity. A better understanding of the consequences of local cyber insecurities on the global commons is needed. This would help prioritize the investments needed for capacity-building while weighing international and local interests. Research exploring states’ nonconformance with norms and different norm-development processes has been started and needs to be furthered.31

2. Recognize the Different Valuations of Risks—but Weight Effects on the Global Commons

Just as states did not initially and fully appreciate the potentially catastrophic nature of WMD proliferation risks, many today do not understand the potential enormity of risks that cyber and other emerging technologies such as AI present. Building value propositions around security and accountability for implementation of norms and laws is important. States have such wide-ranging needs that capacity-building is necessary to foster development along with security.

Recommendation: The true value proposition in investments in compliance with cyber norms and international law has not yet been made clear, and common interest in global cybersecurity needs to be strengthened. Local interests will differ among countries but must take account of the knock-on global effects that local decisions can have for issues like cyber and malicious ICT activity. A better understanding of the consequences of local cyber insecurities on the global commons is needed. This would help prioritize the investments needed for capacity-building while weighing international and local interests. Research exploring states’ nonconformance with norms and different norm-development processes has been started and needs to be furthered.32

3. Incentivize Performance

UNSCR 1540 has no enforcement mechanisms but relies on incentives for states to report and conform to the resolution’s obligations. The Committee leverages the work of other institutions that require interrelated reporting. The reporting and committee internal reviews incentivize compliance by encouraging transparency, trustworthiness, and more international accountability. Using the UNODA trust fund and working through assistance providers and other international organizations have helped implementation.
Recommendation: Supporting implementation and reporting, linking implementation to developmental goals, and providing funding for these efforts are all key to advancing compliance with cyber norms and laws. Existing organizations’ efforts in cyberspace can be better coordinated and harnessed in the digital domain. However, possible consequences from nonconformance with resolutions, norms, and laws also need to be discussed and articulated.

4. Adapt, Coordinate Efforts, and Lead

The Security Council believed that efforts to address WMD proliferation could be strengthened, expanded, and monitored centrally via the work of the 1540 Committee and its Group of Experts in cooperation with states and civil society. The Committee recognizes it now needs to review its work and the matrix to adapt to new and emerging needs and that this will take expert input and leadership. In the 1540 context, leadership could be provided by a wide range of actors: the Committee chair, member states that lead working groups, the local contacts in states and now regions, and the larger UN system of organizations. The local contacts and the COE have not reached their full potential due to states’ disagreement over their proper role and functions. The UNODA’s role in supporting regional leadership and its use of the voluntary trust fund for implementation has helped counterbalance some of the Committee’s challenges.

Recommendation: International leadership is needed to help reduce cyber risks and promote cyber norms and laws. While central coordination of the many ongoing efforts to promote cyber stability and reduce threats is needed, the challenges of UN coordination must be acknowledged. A recent UN policy brief from the UN Secretary-General highlights the need for new governance frameworks to mitigate harm and address cross-cutting risks. This includes consideration of how new digital technologies may be applied to multiple threats, such as in the biological and nuclear areas and calls for new mechanisms for accountability. The proposed Cyber Programme of Action should ensure that the proposals being put forward are implementable and that there are clearly defined roles and responsibilities for all stakeholders.
Endnotes


3 The United Nations Security Council, with its 15 member states, passes many resolutions every year. To pass a resolution, nine votes are required without a veto from any of its permanent members (China, France, Russia, the United Kingdom, the United States). Unlike resolutions of the UN General Assembly, Security Council resolutions can be binding if evoked under the Chapter VII “threat to international peace and security” provision of the UN Charter, thereby imposing obligations on member states. When a Security Council resolution (UNSCR) is passed under Chapter VII of the charter, concerning threats to international peace and security, the Council “decides” that states must take some specific actions.


Note UNSCR 1977 (2011) also asked the 1540 Committee, with assistance from the group of experts, to “identify effective practices, templates and guidance, with a view to develop a compilation, as well as to consider preparing a technical reference guide about resolution 1540 (2004), to be used by States on a voluntary basis in implementing resolution 1540 (2004), and in that regard, encourages the 1540 Committee, at its discretion, to draw also on relevant expertise, including, civil society and the private sector, with, as appropriate, their State’s consent[.],” available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1977%2520(2011)&Language=E&DeviceType=Desktop&LangRequested=False.


United Nations, 1540 Committee, “National Points of Contact,” available at: https://www.un.org/en/sc/1540/national-implementation/national-points-of-contact.shtml. Often the states’ official point of contact with the Committee, which is publicly available, will facilitate reporting, although a survey found that many had difficulty in reporting and were not clear on their roles. The survey reached 105 of the 123 states with points of contact in 2020 and received 34 replies. Seema Gahlaut, “1540 Points of Contact: An Underutilized Resource,” The Stimson Center, August 1, 2022, https://www.stimson.org/2022/1540-points-of-contact-pocs-an-under-utilized-resource/.

United Nations, Office for Disarmament Affairs, “Training Courses,” https://www.disarmamenteducation.org/index.php/go-education#online. Often the states’ official points of contact with the Committee, which are publicly available, will facilitate reporting, although a survey found that many had difficulty in reporting and were not clear on their roles.


VERTIC (the Verification Research, Training and Information Centre) developed toolkits for states to use in legislation complying with obligations under 1540, including as part of the BWC, CWC, and other nuclear/radiological agreements. The Stimson Center initiated a pilot project that provided pro bono support from lawyers and from law school and graduate university students to develop prototype legislation and explain the benefits of better trade controls, with a focus on the Caribbean. Stimson also assists in supporting implementation and publishes a roster of support resources and developed a student essay contest to promote international awareness among students and others in academia.

The Center for International Trade and Security for a number of years published the journal 1540 Compass that shared ideas on effective 1540 implementation, https://disarmament.unoda.org/.


Yet, it was not until 2012 that FATF adopted specific guidance on proliferation financing and the need to address that in the context of 1540 requirements. Council of Europe, Resolution Res (2005), 47, https://www.coe.int/en/web/moneyval/implementation/financing-proliferation.


Designing a solution is easy. It is implementing the solution, which takes great effort to succeed. Similarly, multilateral framework solutions are only as effective as the strength of the partnerships and implementation efforts to sustain them.

This case study examines what governance mechanisms and capacity-building initiatives are functioning well in outer space and proceeds to make the case for how these measures might be applied toward promoting accountability in cyberspace. Could there be an outer space ‘skeleton key’ for ‘unlocking’ accountability in cyberspace?

In exploring this question, the main areas examined in this case study are: (1) the Artemis Accords principles and program; and (2) capacity-building mechanisms for the long-term sustainability of space activities. Global capacity-building activities are beneficial because they help foster conditions for states to cooperate on shared goals and can strengthen forming a rules-based international order.

Outer Space Governance

First, it is important to introduce relevant legal framework to better appreciate the origin story of the Artemis Accords principles. The 1967 UN Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (OST) is the seminal document for outer space law. The OST is a leading document that prohibits national claims of sovereignty, the establishment of military bases and weapons, or the placement of weapons of mass destruction (WMD) in orbit or on celestial bodies. Another significant treaty is the 1972 Liability Convention, which is an agreement for states to take full responsibility for any damages caused by their space objects. This 1972 treaty is currently being tested however, by the rapid rate of technological advancements of the civil space sector. Traditionally, the law is slower in evolving to respond to technological developments, however, identifying the legal gaps and barriers is a necessary exercise to cultivating a robust accountability ecosystem.

Together, these legislative instruments signify that accountability of states is a concrete reality in space and not just broad political principles. Through both the OST and the Liability Convention, states bear legal and financial responsibilities for public and private national space activities. Overall, the OST, combined with the United Nations (UN) Charter and other relevant international laws, represent “the essential framework for the peaceful exploration and use of outer space for the benefit of all nations.”

* The opinions expressed here are solely those of the author.
Case Study 1: The Artemis Accords’ Principles and Lunar Program

This section focuses on the Artemis Accords principles. It proceeds to draw connections between how certain aspects of the Artemis lunar exploration program could be applied to promote accountability in cyberspace among states.

The Artemis Accords are composed of nine nonbinding principles that are drawn from the OST and other international laws. The Accords champion the peaceful exploration and scientific research of outer space, as well as advance the safety and sustainability of space activities. These principles of state cooperation for the peaceful uses of space are displayed in the table below.

<table>
<thead>
<tr>
<th>The Artemis Accords’ Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peaceful Exploration of Space</td>
</tr>
<tr>
<td>Preserving Space History &amp; Heritage</td>
</tr>
<tr>
<td>Transparency</td>
</tr>
<tr>
<td>Space Resources</td>
</tr>
<tr>
<td>Interoperability</td>
</tr>
<tr>
<td>Deconfliction of Activities</td>
</tr>
<tr>
<td>Emergency Assistance</td>
</tr>
<tr>
<td>Orbital Debris</td>
</tr>
<tr>
<td>Registration of Space Objects</td>
</tr>
</tbody>
</table>

**APPLYING ARTEMIS TO ACCOUNTABILITY IN CYBERSPACE**

At the time of writing, there are 39 state signatories to the Artemis Accords. The most recent signatory is Slovenia on April 19, 2024. The other signatories include Angola, Argentina, Australia, Bahrain, Belgium, Brazil, Bulgaria, Canada, Colombia, the Czech Republic, Ecuador, France, Germany, Greece, Iceland, India, Israel, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Nigeria, Poland, the Republic of Korea, Romania, Rwanda, Saudi Arabia, Singapore, Spain, Sweden, Switzerland, Ukraine, the United Arab Emirates (UAE), the United Kingdom (U.K.), the United States (U.S.), and Uruguay.

Apart from the Accords principles for advancing responsible state behavior, the Artemis lunar exploration program is also a capacity-building measure. Simply put, it operates as a mechanism to build partnerships and foster cooperation for lunar and deep space exploration with spacefaring nations. The Artemis program was established in October 2020 by coalition partners from Australia, Canada, Italy, Japan, Luxembourg, the UAE, the U.K., and the U.S.

The Artemis Accords Coalition (i.e., the 39 state signatories) is also interested in exploring beyond the moon and showcasing global partnerships in promoting the safe and sustainable uses of outer space for future generations. With 39 state signatories, the Artemis Accords enjoys generally positive global reception. For example, the president of the Polish Space Agency (POLSA) praised the Accords for promoting space collaboration and transparency, observing that POLSA was “very proud that we have members from all continents now.”
Support for the Artemis Accords, however, is not without its challenges, particularly stemming from the provision about the deconfliction of space activities through the establishment of “safety zones.” Some scholars have critiqued this aspect of Artemis as “an attempt by the Americans to walk softly to legitimize their deviation from the Outer Space Treaty.” At the same time, these principles, such as emergency assistance, registration of space objects, and preserving space history, are not radically different from what is already enshrined in the OST, as well as several core supporting agreements, such as the Rescue Agreement, the Liability Convention, and the Registration Convention. (See Appendix I).

Several of the Artemis principles are relevant for accountability, including in cyberspace. For instance, the principle of transparency—widely viewed as integral to accountability—recites that signatory states should conduct their activities in a peaceful and transparent way. To build transparency, the principle recommends that “Artemis Accords signatories commit to the public release of scientific information, allowing the whole world to join us on the Artemis journey.” This recommendation manifests in a variety of ways. One example is that during the formal ceremonies where states accede to the Artemis Accords, the incoming state publicly pledges to uphold a rules-based approach for the scientific exploration of space and to share information and resources toward a unifying space exploration goal.

Focusing on information sharing, the Artemis Coalition partners have convened two informal working group sessions as of this writing. The president of the Japan Aerospace Exploration Agency (JAXA) who also served as one of the co-chairs of the Coalition’s Working Group One in 2022 described the goals of these sessions as establishing partnerships for information sharing for near-term civil lunar mission plans and transparency to reduce mission deconfliction in lunar surface activities.

The U.S. Combined Space Operations Center’s Space Surveillance Network tracks manmade space objects currently orbiting the Earth. Orbital debris poses a challenge to space sustainability, and therefore, space governance. Illustration by NASA Orbital Debris Program Office.
The group’s first session was informally convened in 2022 to discuss how the Artemis Coalition could promote a multilateral dialogue on mission deconfliction and transparency in space activities. Under the aegis of the Artemis Accords framework, several Artemis parties met as a working group again in Baku, Azerbaijan, in 2023. This was the second working group meeting of the Artemis Accords signatories and coincided with the 74th International Astronautical Congress held in Baku. At this working session, the parties discussed how to promote transparency, ensure safety in civil lunar surface operations, and reduce the risk of misunderstanding. At the time of writing, it has not yet been announced if a third informal working group session will be convened at the forthcoming 75th International Astronautical Congress in Milan, Italy, in October 2024.

One benefit of these Artemis-led informal working group sessions is that they have the potential to be a means to publicly acknowledge and praise states for their transparency in space activities. For example, during the session in 2023, the NASA Deputy Administrator praised India for leading by example by exhibiting the Artemis Accords principle of transparency with its Chandrayaan-3 lunar landing mission. “They showed everything. They let the world join them online to watch the progress of this event….And in so doing, they upheld the highest principles of the Accords,” said Melroy. As this report highlights, positive reinforcement is an incentive for states to comply with norms of responsible state behavior in outer space. To comply with the peaceful use of space, a positive reinforcement mechanism could be informal Artemis working group sessions at the International Astronautical Congress. A working group session may be a good model for positive encouragement with respect to the transparency and operationalization of the UN Framework for Responsible State Behavior, in particular the eleven nonbinding norms.

In support of transparency, the UN also maintains the world’s largest online and publicly available Register of Objects Launched into Outer Space. While it is not a panacea, this open registry system helps promote transparency because this type of information sharing builds trust among nations and enables better communication for the secure operation of space missions and traffic management.

The notion of deconflicting activities in a shared space or “global commons” could also be relevant for cyber-related activities of states. Deconfliction of space activities is also one of the nine Artemis principles. These types of activities include, but are not limited to, information sharing on mission length and the expected launch and lunar landing dates. Another governance aspect is the obligation to report the registration and launch of space objects. This principle is a requirement set forth in the 1976 Registration Convention. Under the convention, states are required to provide timely data to the UN on all objects launched into space. The relationship between this principle and the Convention demonstrates the mutually reinforcing relationship between laws and norms in outer space governance. A parallel initiative could be explored to encourage information sharing as it pertains to bolstering national, regional, and global Computer Emergency Response Teams (CERTs) to respond quickly to malicious cyber activity, such as a ransomware attack against another nation’s bank or hospital.

The origin story of the Artemis Accords principles may also be relevant and instructive for cyber accountability, because it demonstrates how unilateral positions and actions can bring states together. In turn, these opportunities for collaboration at times develop into coalitions of like-minded governments rallying together around specific threats or challenges. This collaboration advances accountability because states can form coalitions to discuss actions in line with existing international law, when it might otherwise be challenging to do so within other forums. For instance, the efforts of the U.S. to lead a ban on direct-ascent anti-satellite tests (ASAT) are another example from outer space governance of how pledging to
refrain from a certain type of behavior could help encourage other states to follow suit in making a similar commitment. Further, the subsequent UN General Assembly (UNGA) resolution adopted in support of the ASAT ban may not have legal weight but does show how customary norms are formed and how nonlegal mechanisms can be used to reinforce what is regarded as unacceptable behavior.

Given the low likelihood of a comprehensive cyber security treaty being adopted soon, initiatives like these may be a more viable option to move the needle of progress higher for accountability.

**APPLYING ARTEMIS ACCORDS PRINCIPLES TO QUANTUM COMPUTING CONCERNS?**

To encourage states to develop an agreed normative framework for quantum-based technology, the government of Switzerland and the Geneva Science and Diplomacy Anticipator is unveiling the Open Quantum Institute in Geneva, at the European Organization for Nuclear Research (CERN). Quantum computers are advanced computational machines that use information storage units called quantum bits—qubits—and can solve complex mathematical problems exponentially faster than digital computers.  

The Artemis Principles could provide a useful basis for discussions between the Open Quantum Institute and global stakeholders, as initiated in March 2024.  

This three-year initiative will formally become part of CERN’s global outreach program with the Quantum Technology Initiative (QTI). Combining resources, the Open Quantum Institute will be CERN’s de facto “societal arm” to convene a global diplomatic dialogue on quantum computing and support the UN Sustainable Development Goals (SDGs).  

Multilateral governance frameworks for quantum computers could act as a means for states to protect their sovereign authority in building accountability in the peaceful use and exploration of quantum computing. Sovereign authority in technological environments that transcend physical boundaries is generally referred to as “digital sovereignty.”

Increasingly, states and international organizations like the UN and the North Atlantic Treaty Organization (NATO) are concerned about the potential security risks posed by quantum computers. The UN Secretary-General cautioned the UNGA in 2022 that quantum computers could potentially “destroy cybersecurity and increase the risk of malfunctions to complex systems. We don’t have the beginnings of a global architecture to deal with any of this.”  

Although the Open Quantum Institute is in its incubation phase, its leadership is already coordinating with 130 partners to explore governance approaches for the responsible use of quantum technology, noting that there is an equally “strong need for international cooperation in order to preserve human agency, accelerate our progress towards the SDGs, and ensure that the whole world contributes to and benefits from quantum computing.” This situation is an opportunity for the policy and scientific global community to come together to discuss how to advance accountability mechanisms for the observance of agreed cyber norms for quantum-based technology.
Case Study 2: Promoting Accountability Via Capacity-Building

Cyber capacity-building activities help foster the conditions to engage the international community in upholding and strengthening a rules-based order in cyberspace. Capacity-building has been underscored as crucial for accountability, notably positive accountability.

Capacity-building activities to support long-term sustainability in space are generally understood in reference to enhancing the ability to operate in space in the future. Within international fora, it is defined as operating “in a manner that realizes the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes.” This definition is based on the 2019 Guidelines for the Long-Term Sustainability (LTS Guidelines) of Outer Space of the United Nations Committee for the Peaceful Uses of Outer Space (UN COPUOS). Surprisingly, the LTS Guidelines do not mention cybersecurity, which is an essential component for supporting the engineering life cycle of developing sustainable, secure, and resilient space systems. As a mechanism to generate accountability, this oversight could be an opportunity to promote global cooperation for identifying best practices and standards for safeguarding space assets and their supporting infrastructure from cyber threats. While the international LTS Guidelines are voluntary, international cooperation by states and global organizations to comply with the LTS Guidelines aligns with furthering another global framework—the SDGs—as it relates to the climate and the sustainability of space operations for future generations.

Finally, space offers other good models of capacity-building initiatives that could have relevance for cyber and accountability more broadly because of how they bolster transparency and information sharing. Specific examples include but are not limited to:
• Space Situational Awareness (SSA) mechanisms like the United Nations Office for Outer Space Affairs’ UN-Spider Portal, which is a common repository of technical capabilities (software) necessary to interpret space data. By sharing capabilities to monitor space activities, actors can verify compliance and hold disrupters accountable.

• The Space Track platform, which is a unilateral initiative to offer a freely accessible service to monitor activity in Earth's orbits.

• Direct investments in connectivity and space infrastructure to promote cybersecurity, increase resilience, and reduce the risk of redundancy in architectural design.

OTHER CONSIDERATIONS

It cannot go overlooked that there is a deepening relationship between outer space and cyberspace, which may require that cyberspace has its own governance and accountability mechanisms or better integration and application of existing outer space norms and laws. Events at the outbreak of the Russia-Ukraine war underscore well the need for further review of the relationship between cyber- and outer space. There has also been a growing use of cyber and electronic “counter space weapons.”

Cyber counter space weapons can take a variety of forms and consist of activities including intercepting and monitoring data, corrupting data with malware, or even wresting control of the space system from the space operator. These weapons can disrupt and degrade the functionality of systems and, in extreme cases, destroy them. The Ukraine war demonstrates how malicious cyber actors can manipulate several points of entry to exploit ground-based, as well as orbiting, systems.26

During the UNGA First Committee session in October 2022, a Russian foreign ministry official declared the U.S. use of commercial satellites in the Ukraine war to be “provocative” and questionable under international space law. He warned that “quasi-civil infrastructure may be a legitimate target for a retaliation strike.”27 Despite this announcement, there is no bright-line rule under international law for targeting dual-use satellites. In fact, targeting commercial space satellites that support both military and civilian populations implicates an array of legal commitments alongside informal ones, such as international telecommunications law, international space law (such as the OST), and even nonbinding guidelines regarding space debris mitigation.

At a meeting of the 2023 UN Open-Ended Working Group (OEWG) on Reducing Space Threats Through Norms, Rules and Principles of Responsible Behavior meeting, the U.S. representative explained that the dual-use nature of an increasing number of space systems presents a challenge to devising a durable definition for what constitutes a “weapon” in space.28 The U.S. representative also expressed concern that some actors might claim civilian satellites are “weapons” as a subterfuge for targeting them on political grounds.29 Just as the Woomera Manual30 is envisioned to support a rules-based order for military space activities during periods of tension and armed conflict, global policymakers must be prepared to address the complex issues that traverse cyber and space in order to advance accountability.
Key Takeaways and Recommendations

As this case study has explained, there is a deepening relationship between outer space and cyberspace, which may require that cyberspace has its own governance and accountability mechanisms or better integration and application of existing norms and laws for outer space.

1. Designing Governance Mechanisms that Span Cyber and Outer Space

Global policymakers must be prepared to address the complex issues arising from the convergence of space and cyberspace threats; particularly as the use of cyber and electronic counterspace weapons increases. There is a need to better integrate cyber-related threats and concerns within outer space mechanisms and frameworks, and vice-versa. International cooperation will become “even more important as both the opportunities in space evolve and the threats, in and to space, evolve as well.”

Given the cross-domain connections between cyberspace and outer space, it is reasonable to examine what strong mutual priorities are functioning well in space and see if they might be similarly suited for building consensus around observing global cyber norms.

For example, the LTS Guidelines described earlier do not mention cybersecurity. This is an essential component for supporting the engineering lifecycle of developing sustainable, secure, and resilient space systems. As a mechanism to generate accountability, this support could be an opportunity to promote global cooperation for identifying best practices and standards for safeguarding space assets and their supporting infrastructure from cyber threats. While the guidelines are voluntary, international cooperation by states and global organizations to follow these guidelines is in alignment with realizing several of the goals articulated in the SDGs as it relates to protecting the climate and ensuring the sustainability of space operations for future generations.

2. Pledges to refrain from certain actions can help signal cooperation and build trust amongst States to advance joint coordinated action

Collectively, the Artemis Program, the Accords, and the ASAT ban can be relevant to cyber, because these examples demonstrate how coalitions of like-minded governments can advance action to respond to specific threats or challenges in line with existing international law. This approach is particularly relevant when the case might be challenging within established fora or institutions. Starting within a like-minded coalition is often a first step to signaling what is, and what is not, responsible state behavior. Such coalitions can also be more open to the active involvement of nongovernmental stakeholders because of their flexibility and relatively informal status. To some extent this is already happening in cyber through the recently launched Pall Mall Process on commercially available cyber intrusion capabilities or efforts within the Paris Peace Forum and Paris Call for Stability in Cyberspace. A cyber corollary for enabling accountability in the responsible use of cyberspace could be a similar pledge to refrain from other forms of harmful activity in cyberspace, like industrial economic espionage. Overall, accountability can be bolstered when states pledge to refrain from certain forms of conduct and meaningfully take action to signal that commitment to other states.
Endnotes


4. Ibid.

5. Ibid.


12. Ibid.

13. Ibid.

14. Ibid.


Note: In February 2022, actors from the Russian state launched a malicious cyber operation against Viasat Inc.’s KA-SAT commercial satellites, disrupting thousands of modems across Ukraine and Europe. The attack also produced indiscriminate harm by disrupting wind turbines and internet services to private citizens across Europe. There is evidence of the Russian Federation persistently interfering with commercial space satellites supporting Ukraine and, by some accounts, evidence that the Ukrainian Armed Forces air defense units are targeting Russian electronic-warfare units using unmanned aerial vehicles (UAVs) interfering with Ukraine’s satellite communications; specifically, taking down Russian UAVs Horizon Air S-100 and Orlan-10 using Stingers. Electronic counter space weapons disrupt the transmission of radio frequency signals by jamming and spoofing communication relays and interfering with positioning, navigation, and timing (PNT) signals like GPS. On May 10 2022, SpaceX Founder Elon Musk tweeted that the Starlink terminals deployed in Ukraine had successfully “resisted Russian cyberwar jamming & hacking attempts so far, but they’re ramping up their efforts.”


Ibid.


Advancing Accountability in Cyberspace,
Stimson Center

Image by NASA Earth Observatory.
5. The Remarkable Story of the Montreal Protocol with Lessons for Cyberspace

Debra Decker and Kathryn Rauhut

The world responded in a unique and singular way to a problem discovered in 1985 that threatened the global commons: a hole in the ozone layer caused by ozone-depleting substances (ODS) with potentially severe consequences to human health and the environment. The Montreal Protocol is one of the most successful mechanisms addressing international risks. Its achievement underscores the importance of developing common goals, incentivizing compliance, and measuring outcomes to ensure accountability. Important lessons for cyberspace can be taken from studying the development and implementation of global efforts to reduce the risks from stratospheric ozone.

An Evolving Framework

In 1985 the Vienna Convention for the Protection of the Ozone Layer (Vienna Convention) was adopted as a “framework convention”—a steppingstone toward addressing the depletion of ozone in the atmosphere but without requiring direct action. However, the Vienna Convention did obligate states to cooperate in developing “agreed measures, procedures and standards” to reduce ODS emissions with the development of future protocols and annexes to the Convention as science/technology advanced and negotiations continued toward appropriate actions.¹ Two years later, the Montreal Protocol on Substances that Deplete the Ozone Layer (Montreal Protocol) was adopted.²

According to the UN Environment Program (UNEP), “The Montreal Protocol phases down the consumption and production of the different ODS [ozone-depleting substances] in a stepwise manner, with different timetables for developed and developing countries” (with developing countries referred to as “Article 5 countries”). All parties have specific responsibilities related to the phaseout of the different groups of ODS. “Developing and developed countries have equal but differentiated responsibilities, but most importantly, both groups of countries have binding, time-targeted, and measurable commitments.” The Protocol took a phased approach to implementing requirements, which were determined based on their feasibility and with procedures that had been determined at the Convention.

The Montreal Protocol cites controls for groups of substances weighted by ODS potential, with its parties calculating their production, consumption, and trade in those substances. Trade of ODS with states not party to the convention is restricted, with controls based on each state’s national circumstances.
Atmospheric scientists at NASA projected the levels of stratospheric ozone that may have existed if the Montreal Protocol had not been adopted, and if CFCs had not been regulated. By extrapolating to the year 2065, the simulation shows the success of the Montreal Protocol in restoring the Ozone Layer. Illustration by NASA/Goddard Space Flight Center Scientific Visualization Studio.

The Protocol defines the phaseout/controls process, with mechanisms for determining and treating noncompliance decided at subsequent meetings. State parties review the controls at least every four years. Before the review, panels of experts in scientific, environmental, technical, and economic information are convened to assess and report on control measures. State parties are required to report annual ODS data, called Article 7 data, to check on compliance with the control measures.4

The Protocol has been amended five times to reflect new science and concerns, with the most recent being the 2016 Kigali Amendment.5 Researchers recognized the inadvertent impact on global warming that some of the Protocol’s earlier steps were causing, specifically the substitution of hydrofluorocarbons (HFCs) for hydrochlorofluorocarbons (HCFCs) and chlorofluorocarbons (CFCs), which are widely used in refrigeration and air conditioning and are powerful greenhouse gases with global warming potential (GWP) thousands of times higher than that of CO2. The Kigali Amendment phases down global production and consumption of all key HFCs, with exemptions available for critical and/or essential uses.6 It also divides Article 5 countries into two further groups recognizing different baselines reflecting parties’ current levels of dependence on the named substances and allowing different phasedown schedules.7

From the framework established by the Vienna Convention to the Montreal Protocol and its attendant processes, the world has witnessed a slow but meaningful march toward accountability for healing the ozone hole and mitigating climate change, as all ODSs are also greenhouse gases.
Overseeing and Incentivizing Compliance

It took several years of negotiation to develop a noncompliance mechanism for the Montreal Protocol, which was subsequently revised. The mechanism is comprised of an Implementation Committee of 10 State Parties, representing various regions, which is supported by the UN Secretariat. Compliance activities overseen by the Committee include annual reporting of data, phasing out of consumption and production of ODS, and implementing a licensing process including restricting trade with nonstate parties. The naming of State parties that are not in compliance and expressions of concern are what encourage countries to comply.

The Implementation Committee assists countries to meet their implementation targets. This provides positive incentives. Countries self-report their own noncompliance and can seek grace periods and assistance. Verification of data and timeliness of reports have been issues, but the implementing agencies involved—including the UN Development Programme, the UN Industrial Development Organization, and the World Bank—provide some confirmation of data. The Protocol promotes sharing of technological approaches and best practices and evaluates the costs and benefits of different strategies for compliance. Advisory groups on technical options and economic assessments assist State parties. State parties are asked to report every two years on their collaboration efforts and on efforts to educate the public on effects of ozone depletion (Article 9); however, compliance with this request is not monitored by the Implementation Committee so only some countries appear to report, even when they do comply.

An important aspect of the success of the Montreal Protocol is its unique financial mechanism, the Multilateral Fund (MLF) for the Implementation of the Montreal Protocol, which provides technology transfer, institutional strengthening, and financial assistance in both manufacturing and servicing sectors to developing countries. This financial assistance enables these countries to achieve compliance. At first, developed countries were responsible for most of the world’s ODS production and consumption; however, some developing countries, in particular China and India, are now major ODS and HFC producers.

As of November 2023, contributions to the Fund totaled $5 billion. The MLF Executive Committee receives project proposals, oversees disbursements, and evaluates the effectiveness of the fund in phasing out ODS. Causes of project success/failure are assessed for reporting on lessons learned. Implementing agencies report against outcomes. For example, OzonAction, a branch of UNEP, measures progress against nine outcomes (see visual below):
## Nine Major Outcomes

<table>
<thead>
<tr>
<th>OUTCOME 1</th>
<th>National Ozone Units effectively manage their national programmes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUTCOME 2</td>
<td>Article 5 countries report accurate and timely data</td>
</tr>
<tr>
<td>OUTCOME 3</td>
<td>Effective legal, regulatory, and policy frameworks are in place and enforced</td>
</tr>
<tr>
<td>OUTCOME 4</td>
<td>Imports and exports are controlled, and illegal trade is reduced/prevented</td>
</tr>
<tr>
<td>OUTCOME 5</td>
<td>Key stakeholders and the public enthusiastically support national compliance programmes</td>
</tr>
<tr>
<td>OUTCOME 6</td>
<td>Non-ODS, low GWP technology is adopted and used safely, and servicing sector workforce skills are strengthened</td>
</tr>
<tr>
<td>OUTCOME 7</td>
<td>Energy efficiency is maintained or increased in the RAC sector</td>
</tr>
<tr>
<td>OUTCOME 8</td>
<td>Gender issues and approaches are considered and addressed in Montreal Protocol programmes and projects</td>
</tr>
<tr>
<td>OUTCOME 9</td>
<td>Article 5 countries meet their commitments through effective and timely implementation of Multilateral Fund projects</td>
</tr>
</tbody>
</table>

Illustration from [https://www.unep.org/ozonaction/who-we-are](https://www.unep.org/ozonaction/who-we-are).

Incentives for compliance are working. Every four years, a scientific assessment of the treaty’s effects is presented. The most recent one in 2022 found, “Actions taken under the Montreal Protocol continue to contribute to ozone recovery.” Over 200 scientists from 30 countries were involved in the assessment. Although the assessment warned that the Protocol faces many policy and scientific challenges to protecting the ozone layer, the ozone layer is expected to recover by the middle of the 21st century.

The Montreal Protocol regime of agreements and procedures, now in its fourth decade, is adapting to meet new challenges. In 2018, a group of scientists reported increased emissions of CFC-11, which was unexpected given the substance had been banned since 2010. The Environmental Investigation Agency (EIA), a British nongovernmental organization (NGO), released related findings at the 2022 State parties meeting tracing the emissions to the illegal production and use of CFC-11 in China. Given the revelations, China took some early targeted actions to reduce violations, but EIA noted that more oversight was needed worldwide. As some researchers have noted, “…the Montreal Protocol has achieved remarkable success through its flexibility and adaptive responses to scientific and technological advances... It is time for it to adapt again if it is to be a twenty-first century success story.”

### Key Factors in the Development of the Agreement and Its Mechanisms

CFCs were invented in 1928 to replace some other hazardous materials used in homes for refrigeration; by the middle of the 20th century, CFCs were in wide use as a part of air conditioners, plastic manufacturing, and aerosols including hair spray. In the early 1970s, industry and scientists began to suspect the impact of these ODS and their long-lasting impact on stratospheric ozone. Without that layer of ozone filtering out harmful Ultraviolet-B radiation, humans have more eye cataracts compromising vision, more skin cancers and some compromised immune responses; additional adverse effects on plants and marine life have more recently been noted.

The United States (U.S.) was responsible for about one-third of the global consumption and production of CFCs, and industry pushed back against possible controls.
In 1977, UNEP convened an international meeting that agreed to establish a World Plan of Action on the Ozone Layer. In 1981, the UNEP Governing Council asked the UNEP Executive Director to establish a group to start work on a framework convention to respond to environmental concerns about ozone depletion. These actions are what led to the Vienna Convention in 1985, when there was an announcement of the discovery of a hole in the ozone shield over Antarctica and further validated earlier scientific findings. Industry opposition diminished once they recognized the inevitability of controls. Companies changed strategy and researched alternatives—another route to technological and commercial success.

Certain individuals and countries helped drive agreement.

In 1980, Norway hosted a meeting of like-minded countries—Canada, Denmark, Germany, the Netherlands, Norway, Sweden, U.S.—and the European Commission that decided to push for negotiations for a convention. A proposal from Sweden led to the establishment of an Ad Hoc Working Group of Technical and Legal Experts by the Governing Council. This working group began work in January 1982 toward a draft convention. Unable to agree on substance, they proposed a framework treaty, the Vienna Convention.

A group of individuals from Canada, Denmark, Finland, Norway, Sweden, and the U.S. became known as the “the Toronto Group.” The group proposed a resolution to be approved at the same time as the Vienna framework treaty that called for negotiating a follow-on protocol.

UNEP’s executive director facilitated agreements via informal, closed-door discussions. Negotiations were also preceded by informal workshops, including industry representatives for the first time as more than observers. The director asserted that a protocol would be signed in the fall of 1987 and put forth his own proposals based on his confidential discussions with difficult delegates. He is credited with “orchestrating” agreement on a process with clear outcomes. Personal relationships and innovative late-night ideas helped delegates reach agreement.

Professional panels were established for independent scientific, technological, economic, and environmental assessments.

Panel chairs were unconstrained in how they developed committees of experts to contribute to the proceedings. Experts contributed their knowledge; they did not advise on policy but presented options and did not represent governments or industries. The goal was to strive for international representation and information from peer-reviewed journals, and a technology panel sought experts from industry given that new technological assessments were not yet included in peer-reviewed publications. These independent advisers worked collaboratively with experts from developing and developed countries to provide varied approaches to problems to gain international support. Obtaining and assessing data were key. New/better approaches are continually sought, such as initiatives to certify refrigerant technicians/drivers and to move toward the use of natural low and/or very low refrigerants.
Funding schemes, technical support, and flexibility in phaseout schedules attracted countries that were initially opposed.

The London Amendment to the Protocol entered into force in 1992 and required the expeditious transfer of the best available and environmentally safe substitutes and technologies and committed State parties to meeting the agreed incremental costs in order to enable compliance by developing countries. This was a critical factor in getting more States to sign on. Some like India worried about technological dependence on the developed states, who in turn had concerns about intellectual property protections of technology transfers. The ability to have a fund to help finance technological change also attracted countries like China to sign on to the amended protocol.

The public, media, and NGOs played a prominent role in driving agreement.

As one observer mentioned, simplifying the issue and having a dramatic name, “the ozone hole,” captured public attention. Media coverage internationally was uneven, but some significant publications helped inspire change. State parties, as required by the amendment, the UN, and some groups helped raise public awareness, including targeting new audiences such as children. NGOs such as the Natural Resources Defense Council and Greenpeace used legal remedies to advance reduction of ODS.

Reluctant states and industry got onboard.

The potential restrictions on ODS-related trade for those not signing the treaty or falling out of compliance proved to be a significant incentive—in the form of a stick, rather than a carrot—for participation and compliance. In the initial concerns about the ozone hole, the number of actual ODS manufacturers were small, only 15 according to one source. They would have to stop exports to nonstate parties of ODS and items made using these. The adaptive measures allowed—and supported by funding—encouraged states and their commercial sectors to see the benefits of joining and complying with the treaty. In addition to regulatory approaches to controls, some governments imposed taxes/fees on production and/or use of ODS. Some imposed quotas and/or bidding systems for licenses. Product labeling requirements were also introduced in some countries to allow consumer/user pressure on businesses, not just pricing, to help drive change. In addition, and to some extent, government contracts were modified to restrict ODS use/purchases thus leveraging governments’ purchasing power.

Women’s role in driving change becomes recognized.

The role of women in promoting compliance has been recently recognized with the MLF supporting efforts to better recognize gender in programs and assessments and to promote women’s training and participation. Special efforts at capacity-building also target women, for example, providing training and support for women in West Africa to work in refrigeration repair. Implementation of the Protocol can be linked to many of the UN’s Sustainable Development Goals (SDG), including SDG 5 on achieving gender equality and empowering all women and girls.
Relevance to Cyber

The upper atmosphere and cyberspace are both areas where collective action is needed to address cascading effects, the transboundary nature of threats, and the potential harm to the global commons. The long-persistent effects of ODS on the ozone layer made that issue clearly urgent, whereas the harmful scenarios in cyberspace are not universally accepted or always seen as urgent. Although conditions in the world have changed from when the Vienna Convention discussions began, today’s fractured state relations need not stymie progress on cooperation. Even in 1991 when it was a time of difficult transition for the former Eastern Bloc, the former Soviet Union, and the United States, they found they could cooperate to monitor the ozone layer.40

Who can have, and who can afford safer and more secure technologies? The global South and many others at first expressed their basic need for affordable refrigeration and were reluctant to address issues related to ODS. Some, even in developed states, doubted the true effects of ODS and viewed the short-term effects on the economy of disrupting existing industrial practices as too costly. Likewise in cyberspace, the global South and even some in the industrialized North value low-cost, less secure information communications technologies (ICTs) as potentially worth the gains that are possible through quicker, cheaper digitization. Scientists, technologists, and industry experts are critical players in developing solutions to issues in both areas. For ODSs, those discussions and the latitude for compliance are still evolving, even after many decades, given the advances in science and technology—including in monitoring. In cyberspace, that process is still nascent.

Key Takeaways and Recommendations

1. Consider Developing New Technological/Control Approaches

The depletion of stratospheric ozone is a singular well-defined risk that has required new technologies and approaches to be developed and updated as new risks and threats are discovered. Science and investments in research and development supported the transition from agreeing to a framework treaty and protocol to implementation of those instruments. Society, including the private sector, benefited as has the environment.

Unlike ozone, cyberspace presents a multiplicity of problems that largely stem from the underlying risks posed by anonymity. While benefits abound—free, fast information flows with protections for privacy and free speech—cyber anonymity facilitates dis/misinformation and allows shielding of malicious and criminal conduct. As cyber threats have increased with the advent of artificial intelligence (AI) and malware as a service, the risks and threats have multiplied. Artificial intelligence can be applied to help protect individuals, businesses, and governments but that level of sophistication is not widely available.

Recommendation: New approaches for cybersecurity are needed and should continue to be explored, particularly as cyberspace evolves and new technologies generate new threats.

If the digital world could be reinvented today, what would we want it to look like in terms of technologies, access, and controls to better manage cyberspace issues? Could/should new technological approaches and regulations better strike the balance between allowing the benefits of anonymity while finding more ways to ensure accountability as needed?
2. Define the Problem and its Relative Risks

Although the issue of ozone depletion was clear, it was valued differently among stakeholders engaged in the Montreal Protocol process. Negotiation and incentives were needed to reach agreement on common valuations and approaches. The work of international panels of scientists, technologists, and economists informed discussions. Obtaining and measuring data and outcomes from initiatives were all key.

Recommendation: The value placed on privacy versus wrongful use of ICTs differs among and within states and is changing. Reaching agreement on threats and overall risks is challenging. Although discussions at the United Nations (UN) on a broad cybercrime treaty have stalled, important UN discussions on norms and laws for state behaviors continue to help build agreement. Independent panels could perform a more structured analysis of cyber threats and risks, as was done by the expert panels of the Montreal Protocol, to develop a deeper common understanding and definition of incidents and categories of harms. For example, this effort could include estimating the broader societal harms stemming from a state’s actions and inactions in relation to ICT use, such as the potential cascading effects from attacks occurring in their and other countries. Obtaining data and establishing metrics in a consistent fashion are critical. Threat and risk assessments would evolve as information on threats and risks increases and as science, technology, and values change. Policymakers could then weigh conditional risks and their different valuations of harms and trade-offs, then consider collaborative approaches to managing specific risks.

3. Develop Agreed Approaches to Monitoring and Managing Cyber Risks

UNEP was the original hub for assessing and managing ODS risks and systematically involved other organizations in measuring and reporting on the ODS risks—from how the environment was changing to what actions could and might be taken to mitigate risk. Monitoring actions and capacity-building were integral parts of the framework, with an approach that was supportive rather than confrontational. The organizational responsibilities and relationships were complex but clear and mapped out, with supportive accountability mechanisms for managing risks.

Recommendation: In a 2023 policy brief published as part of the process leading to the Summit of the Future to be held later in 2024, the UN Secretary-General called for the establishment of “an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct.” Such a mechanism could not only support accountability and call out malicious uses of cyberspace, but it could also assess and develop recommendations for managing cyber threats as well as monitor implementation and adherence to agreed commitments, including international law and the behavioral norms that comprise the UN Framework for Responsible State Behavior in Cyberspace. It could help develop a structured and consistent approach to collecting data and assessing approaches. This mechanism could also support capacity-building (without duplicating existing efforts) and collectively and systematically evaluate outcomes as is done for ODS projects. The proposed UN Programme of Action (UN PoA) on state use of ICTs could help carry such efforts forward, making current efforts more efficient and effective. The possible harms that pose local, as well as systemic and international risks, could be assessed and should be prioritized to be addressed through capacity-building, regulations, and other approaches. Incentives for compliance are key, especially positive ones with assistance in developing the ability to comply.
4. Support Multilateral Leadership in Developing Agreements With Defined Roles and Responsibilities

The beginnings of agreement on ODS came from like-minded states banding together to take leadership—the Toronto Group. Some usual allies of these states were hesitant to support efforts at first, but with strong leadership from individuals in this group and others, as well as pressures from NGOs, scientists, and eventually the public, more states and businesses came onboard. Informal consultations and workshops outside formal meetings were key to forging relationships and agreements. Clear reporting structures, with separations between governance and implementation, were established among existing and new institutions.\(^{47}\) Regional networks were established to facilitate greater sharing of expertise and reporting.\(^ {48} \)\(^ {49}\)

**Recommendation:** In addressing malicious cyber activity, some states have required leadership to address particular challenges through like-minded coalitions, such as the U.S. initiative on ransomware. Required coordination and leadership goes beyond states however, with cybersecurity firms and others partnering to advance security efforts.\(^ {50}\) However, states and the UN could help focus the efforts of technology firms and others on what they collectively determine to be high-priority needs. Such efforts could lead to developing advisory panels similar in focus to the ODS Technology and Economic Assessment Panel with regional representation. A cyber mechanism could more precisely define what actions demonstrate compliance with agreed norms and international laws. Civil society could help with support as it has in monitoring ozone and other areas.\(^ {51}\)

5. Recognize the Need for Adaptability and Flexibility

The Montreal Protocol demonstrated the importance of adaptability and flexibility in responding to new scientific advancements and emerging challenges—with new solutions and approaches developed. Its negotiation process also recognized that countries with lower socioeconomic development would not be able to adapt as quickly as developed countries. Schedules were modified for those countries and programs were instituted to build their capabilities and positive incentives for compliance—with potential trade restrictions being the penalty for noncompliance.

**Recommendation:** The development and strengthening of cybersecurity norms will likewise require an adaptive process in which all stakeholders will have to continue to be flexible to keep pace with rapid technological advances such as AI and quantum computing. Any new mechanism to address cyber accountability needs to acknowledge this reality.
Endnotes


3 Ibid.


9 Ibid.


13 See, for example, Australia’s “Additional Reported Information” from 2019, on the UN Environmental Programme’s OzonAction profile at: https://ozone.unep.org/countries/profile/aus, whereas the U.S. does not appear to report on outreach but does do this, https://www.epa.gov/ozone-layer-protection/voluntary-educational-and-outreach-programs-related-ozone-layer-protection. See also other observations on Article IX reporting regarding countries’ research and collaboration on pp. 8-9 of the EIA’s briefing to the 34th Meeting of the Parties to the Montreal Protocol (MoP34), “Chemical Nightmare,” October 2022, https://eia-international.org/wp-content/uploads/Chemical-Nightmare-SPREADS.pdf.

The evolving divergence among developing countries in their interest in compliance with the protocol and the Kigali Amendment is investigated in Shiming Yang, “Growing Apart: China and India at the Kigali Amendment to the Montreal Protocol,” Global Environmental Politics 23, no. 2 (2023), 74–101, https://doi.org/10.1162/glep_a_00698.

With nearly $1 billion budgeted for the three years (2024-26), missing info here?, http://www.multilateralfund.org/default.aspx.

The Executive Committee is responsible for overseeing the operation of the Multilateral Fund for the implementation of the Montreal Protocol. The Committee is selected from two groups, comprised of seven members from Article 5 and seven from non-Article 5 parties. They are elected each year by the Meeting of the Parties. Committee decisions are reached by a two-thirds majority vote representing individual majorities of each group—ensuring that neither donors nor recipients dominate the operations of the fund. The chair is chosen from one group, and the vice chair is chosen from the other. Each year they alternate.


Andersen and Sarma, Protecting the Ozone Layer, 44-45.


Andersen and Sarma, Protecting the Ozone Layer, 200-201.

Andersen and Sarma, Protecting the Ozone Layer, 39; 88-91.

Andersen and Sarma, Protecting the Ozone Layer, 442.


Andersen and Sarma, Protecting the Ozone Layer, 438-442.


Andersen and Sarma, Protecting the Ozone Layer, 67.


Andersen and Sarma, Protecting the Ozone Layer, 351.

Andersen and Sarma, Protecting the Ozone Layer, 252-258.


Some headway on this has already been made in limited areas. UN-affiliated and standards development organizations like the International Telecommunications Union and IEEE develop standards especially related to vulnerability management and risk. International Telecommunications Union, “Global Cybersecurity Index,” https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Many different organizations have developed to a large extent organically to fulfill the many needs of cyberspace, such as the Cybil Portal mapping of capacity-building projects and the Geneva Dialogue on Responsible Behavior in Cyberspace coordinating efforts in reducing digital product vulnerabilities in digital products. Government of Switzerland, Federal Department of Foreign Affairs, “Geneva Dialogue on Responsible Behaviour in Cyberspace.” https://genevadialogue.ch/.

See Appendix.


Some headway on this has already been made in limited areas. UN-affiliated and standards development organizations like the International Telecommunications Union and IEEE develop standards especially related to vulnerability management and risk. International Telecommunications Union, “Global Cybersecurity Index,” https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Many different organizations have developed to a large extent organically to fulfill the many needs of cyberspace, such as the Cybil Portal mapping of capacity-building projects and the Geneva Dialogue on Responsible Behavior in Cyberspace coordinating efforts in reducing digital product vulnerabilities in digital products. Government of Switzerland, Federal Department of Foreign Affairs, “Geneva Dialogue on Responsible Behaviour in Cyberspace.” https://genevadialogue.ch/.

See Appendix.


Developing countries have Ozone Contact Units that manage the local program and interface with MLF and others. https://www.unep.org/ozonaction/networks/national-ozone-unit-contacts.


6. The Cyber World and Human Rights: Perspectives on International Accountability

Rosa Celorio

Introduction: Human Rights and Digital Spaces

The United Nations (UN) and regional institutions have been documenting human rights violations occurring in the digital realm, especially since the onset of the COVID-19 pandemic. The digital space includes computers, cell phones, the internet, virtual communications platforms, social media outlets, and artificial intelligence (AI). Even though technology has allowed for the creation of additional online spaces for many individuals to participate and communicate socially, it has also become the setting of alarming human rights violations. These include acute forms of violence, discrimination, hate speech, harassment, bullying, and cyberattacks, all requiring different responses. Many of these human rights breaches are perpetrated not only by state entities, but also a range of private actors. This is noteworthy as we have recently celebrated the 75th Anniversary of the Universal Declaration of Human Rights (hereinafter “Universal Declaration”), still a cornerstone document, but one that could have never anticipated many modern challenges such as cybersecurity concerns and their human rights implications.

International human rights law (IHRL) is mainly composed of a body of legal rules adopted at the supranational level. Most of these rules and their supervisory institutions were conceived to restrain abuse of government activity. The foundations were established in the post-World War II world, propelled by the immense human suffering and toll which resulted from this global conflict. Several rules that we still invoke are part of the Bill of Rights, integrated by the Universal Declaration and the International Covenants on Civil and Political Rights and Economic, Social, and Cultural Rights (hereinafter “the Covenants”). Today we have a set of treaties, under which more than 150 countries have assumed obligations detailing what they will do and not do to prevent human rights violations, but also to affirmatively build societies in which human rights are protected. Some of these are general—like the Covenants—but others are specialized, such as the Convention on the Elimination of Discrimination against Women (CEDAW), the Convention on Racial Discrimination (CERD), and the Convention on the Rights of the Child (hereinafter “CRC”). Strong regional human rights protection systems have also been established in Europe, the Americas, and Africa, governed by their own regional human rights treaties, and evidenced in their prolific work, case decisions, and statements.

Treaties are particularly noteworthy in this framework, as they are considered primary and binding sources of legal obligations for states. When states adopt and ratify human rights treaties, they voluntarily assume a mandate to respect, protect, and uphold human rights. Current treaties protect a range of rights related to life, personal integrity, privacy, dignity, access to information, freedom of expression, and access to justice. The UN has established several organs—referred to frequently as “treaty-based
Connection Between Human Rights Concerns and Cyberspace

The digital age is currently transforming the field of human rights and its norms. Global and regional bodies are now carving out their responses and approaches to human rights violations taking place in cyberspace. The UN General Assembly (UNGA) and the UN Human Rights Council (HRC) have adopted several resolutions expressing concern over the activity of public and private actors in the areas of surveillance, hacking, and AI; encouraging human rights compliance and respect for the rights of all individuals to live free from discrimination and violence; and confirming that international law is applicable in cyberspace.

This is a highly evolving area of the law, with many future developments to come. One critical dichotomy that international human rights bodies are exploring is the fact that digital technologies, such as the internet, have become central to the exercise, defense, and enforcement of human rights, including those related to participation, association, information, and freedom of expression. However, the digital space has also turned into another scenario in which human rights violations take place, including forms of violence, discrimination, and threats to meaningful participation.

It is important to underscore that a set of UN norms has been crafted promoting that states protect human rights in cyberspace and to encourage the respect of UN resolutions in this area. The UN Norms for Responsible State Behavior in Cyberspace (hereinafter “UN Norms” or “UN Cyberspace Norms”) are critical in recognizing that international law applies to state conduct in cyberspace. The sixth and most recent UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) provided further guidance to states on how to operationalize this specific set and other norms. The GGE guidance outlines that states need to respect and protect human rights both online and offline, including freedom of expression, access to information, the right to nondiscrimination and the eradication of the gender digital divide. States are encouraged to invest in technical and legal measures to guide the development and use of information and communications technologies (ICTs) in an inclusive and accessible manner, benefitting marginalized communities and groups.

An important goal in the design of these norms was the preservation of international peace and security as well as the promotion of the safety and well-being of individuals. Voluntary norms of this kind can also lead to state cooperation to act proactively to respect and ensure human rights in cyberspace, by promoting an “open, secure, stable, and accessible ICT environment.”

In addition, the GGE has recognized a range of malicious criminal activity, which is increasingly occurring in digital spaces, including terrorism perpetrated by both state and nonstate actors and arbitrary mass surveillance. The GGE also emphasized that the implementation of the UN Cyberspace Norms should
be consistent with the UN Charter and other binding international law treaties. Norms—even when they are voluntary and nonbinding—can be salient in setting standards for responsible behavior from state and nonstate actors and the expectations of the international community.

In addition, the rules already codified in the human rights framework—in treaties and other legal instruments—apply to the cybersecurity realm. Therefore, the human rights approach to cybersecurity concerns does not begin from zero when it comes to binding obligations. There are key treaties and interpretative guidance that have already been identified as relevant to the digital realm and cyberspace, which protect freedom of expression, access to information, privacy, data protection, property, equality and nondiscrimination, and the right to be free from violence.

The cyber realm does have the added challenge of engagement by many nongovernmental actors, which IHRL was not designed to address. However, international principles—including both binding rules and voluntary norms—have been evolving to address these challenges and identify a set of responsibilities and remedies when needed.

Even though these reflections are mostly centered on the IHRL framework, there are other relevant areas of international law that can be useful to regulate cybercrime and address cybersecurity threats. These areas include international criminal law, which has the goal of bringing accountability and justice to perpetrators of some of the most alarming human rights violations and cybercrime, including genocide, crimes against humanity, war crimes, and crimes of aggression. The International Criminal Court has recently issued several arrest warrants in the context of Russia’s invasion of the Ukraine revealing its potential to prosecute cybercrime in the future.

Indeed, concern about the potential negative impacts on human rights from cybercrime has been central in the negotiations of a global cybercrime treaty at the UN. This process began in UNGA’s Third Committee, which is responsible for the protection of human rights. In 2021, an Ad-hoc Committee (AHC) was established by resolution and tasked with developing a “comprehensive international convention on countering the use of ICTs for criminal purposes.” Over the course of the treaty’s negotiation, it has become evident that member states have very different views on how, and even if, human rights will be protected by a future treaty.

International humanitarian law is also noteworthy, including rules of what can be done or not done during an armed conflict, such as the distinction between civilians and combatants, the principles of necessity and proportionality, and the prohibition to inflict unnecessary suffering.

One avenue for improving cyber accountability may be through the Universal Periodic Review procedure (hereinafter “UPR procedure”) of the UN HRC. As part of the UPR procedure, all UN member states report periodically before the HRC on their human rights records and interventions to respect, protect, and fulfill human rights. The UPR working group examines the following documents during its review: a national report prepared by the state involved; already-issued reports by UN special procedures and civil society organizations; and information presented by national human rights institutions and civil society entities. Within this process, states have an interactive and peer-review dialogue that leads to recommendations to each state on how to improve their human rights record. Several states have already been the subject of recommendations encouraging the adoption of policies to ensure cybersecurity on the internet, which will surely increase in the future given the magnitude of the problems involved.
Key Takeaways and Recommendations

This chapter proposes that current human rights accountability mechanisms can serve to shape state behavior to address cybercrime and cybersecurity concerns. These mechanisms can also motivate states to respond to these crimes as a priority human rights issue, which is meritorious of the states’ legislation, policies, and an adequate justice response. It is important to acknowledge the limitations of these mechanisms, including delays, scarce human and financial resources, the influence of politics, and compliance issues. Therefore, the author suggests the use of human rights accountability mechanisms as only part of the strategy to address concerns related to cyberspace.

The UN charter-based and treaty-based organs are already addressing issues concerning cybercrime and the need for human rights accountability as a priority concern. Important examples are the UNGA and HRC resolutions in this realm, as well as the norms for responsible state behavior in cyberspace. These instruments—even though considered forms of “soft law”—can place important pressure on states to develop interventions at the national level to respond to and prevent these crimes as part of their human rights agenda.

There is scope to better integrate concerns about cybersecurity and cybercrime within existing human rights peer-review mechanisms, such as the UPR. It may also be relevant to consider developing a similar model to evaluate operationalization of the UN cyber norms for example, respecting their voluntary nature, or to use peer review in the development and use of offensive cyber capabilities according to international law.

The current focus on digital violence against women, children, and minorities is also noteworthy and will surely grow in the future, as there is a better understanding of the features of these human rights violations and their impact on groups who are historically marginalized and often victims of discrimination.
Important UN HRC procedures, such as the UN Rapporteur on Violence against Women, have documented the vulnerability of women and girls to digital attacks, including cyberbullying, revenge porn, and hate speech. Such documentation is crucial for ensuring accountability and fostering transparency by building the evidence base and shaping collective understanding about what is, or is not, acceptable cyberspace behavior. These protections are particularly acute for women and girls who voice their opinions in social media outlets and who undertake activities as politicians, journalists, and human rights defenders. Establishing and refining terminology is an area in which the UN Charter and treaty-based organs can make critical contributions to these protection efforts, and they have already begun doing so when addressing digital threats to the human rights of these groups.

The UN Charter and treaty-based organs should continue urging states to prioritize cybersecurity and protect critical rights in an insecure internet environment, including life, personal integrity, participation, freedom of expression, privacy, and others. These groups can sound the horn on the human rights implications of problems such as internet shutdowns, hacking, terrorism, the misuse of AI, arbitrary mass surveillance, and violence in the realm of social media. Cybercrime will more than likely be prominent in future human rights analysis, which will require regulation to reaffirm the need to protect freedom of speech and the free flow of information. Laws and regulations adopted to advance cybersecurity can also inform the future development of international legal standards, benchmarks, and best practices in this area.

The creation of new human rights mechanisms can also occur at the UN level. The UN HRC frequently establishes new procedures to address emerging human rights issues, as it recently did with privacy and climate change. It could potentially create a working group on human rights and technology, which could produce important analysis on the connection between cybercrime and human rights and identify best practices and challenges in state behavior. Current UN initiatives like the Global Digital Compact can support the identification of human rights issues and needed steps to take for both state and nonstate actors on how to address these challenges most effectively.

The zero draft of the compact emphasizes that states should refrain from the use of internet shutdowns, for example. If retained, how to operationalize that commitment could be further fleshed out.

States can also propose to adopt new treaties or protocols to existing treaties, but adoption and ratification processes can be lengthy and onerous, which can impede real effectiveness. Any new human rights treaty developed in this field needs to be proportional in its provisions and respect critical human rights, such as freedom of expression, access to information, and privacy. Given the challenges in adopting new treaties, another alternative is to work with existing treaties and develop interpretations of the applicability of their provisions to cyberspace and cybercrime. The UN and regional bodies working on issues concerning human rights protection in the digital realm can issue in the future interpretative guidelines and resolutions addressing cybersecurity concerns.

Lastly, it is key to underscore the potential of individual case petition mechanisms—popular at the level of UN treaty-based organs and in the regional human rights systems in the Americas and Europe—when human rights violations take place in cyberspace at the national level. These mechanisms can provide a second avenue of justice when domestic judicial institutions fail to adequately respond to human rights violations. Cases have already been presented before regional entities such as the European Court of Human Rights, which evidence the potential for case litigation to promote accountability for crimes related to the use of technology and taking place in cyberspace.
Endnotes

1 See, for example, United Nations High Commissioner for Human Rights, Human rights should be at the heart of tech governance. Number record here? Stimson SG ex “SC/11018,” Sept. 1st, 2022, Human rights should be at the heart of tech governance | OHCHR.

2 For a broad overview, see United Nations High Commissioner for Human Rights, Building a common front against the digital dimension of violence against women. Number record here, if press release, March 15, 2022, Building a common front against the digital dimension of violence against women | OHCHR; Human Rights Watch, It’s time to treat cybersecurity as a human rights issue (March 26, 2020), It’s Time to Treat Cybersecurity as a Human Rights Issue | Human Rights Watch (hrw.org).


In the context of this article, “rules” refer to binding or mandatory obligations assumed by states in the context of a diversity of treaties, legal instruments, and international customs. “Norms” are used to refer instead to principles agreed upon by the international law community of a voluntary nature.


9 For a broad overview of UN charter-based organs and connected institutions, see United Nations System Chart, 23-00013_un_system_chart_11x8.5_print_e.pdf.

10 For examples of recent statements, see Rep. of UN Special Rapporteur on Privacy, Artificial Intelligence and Privacy, and Children’s Privacy, A/HRC/46/37 (Jan 25, 2021), paras. 27-49 (including guiding principles with a human rights perspective on the use of personal and nonpersonal information in AI and its implications on the right to privacy); Committee on the Rights of the Child, General Comment no. 25 on children’s rights in relation to the digital environment, CRC/C/GC/25, March 2nd, 2021, paras. 22-49 (urging states to adopt a range of measures to protect children's rights in technologically driven spaces, including but not limited to the adoption of legislation, policies, strategies, and access to justice).
See, for e.g., the Final Report of the 2013 UN Group of Governmental Experts (GGE) A/68/98 (June 24, 2013), where states first agreed that international law and the UN Charter apply to state conduct in the use of ICTs and reiterated in 2015 and 2021 GGE reports: First Committee Report A/70/455 (Nov. 18, 2015).


Also, G.A. Res. A/RES/78/213 (Dec. 22, 2023), (recognizing the potential for abuse in the digital world and encouraging states to adopt adequate legislation, sanctions, and remedies to protect individuals from human rights violations in this context); UN Human Rights Council Resolution 20/8, A/HRC/RES/20/8 (July 16, 2012), (affirming that the same rights that apply offline, apply online).

See also UN Norms of Responsible State Behavior in Cyberspace, which shed light on what states should do and not do in cyberspace, including human rights protection as a goal, March 2022, The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf (unoda.org).

It is key to note that UN resolutions continue to be adopted in this high-evolving area, including a 2024 resolution on AI, promoting the respect of human rights in its development, deployment, and design. See UN General Assembly Resolution, Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development, A/78/L.49 (March 11, 2024).


See id., page 4, para. 5.


See for example, UN Ruggie Principles on Business and Human Rights, (2011), guidingprinciplesbusinesshr_en.pdf (ohchr.org) (emphasizing the responsibility of businesses to prevent human rights harm and provide remedies when this occurs).


For more information on how the UPR procedure works, see Basic facts about the UPR | OHCHR.


For more discussion of violence against women and girls, which takes place in digital contexts, such as the internet and social media, see Dubravka Šimonović (Special Rapporteur), Rep. of the Special Rapporteur on Violence against Women, its Causes and Consequences, Online Violence against Women and Girls from a Human Rights Perspective, A/HRC/38/47 (June 18, 2018), paras. 12-42.

For more information on the UN Global Digital Compact Initiative, see UN Global Digital Compact: Background Note (Jan. 17, 2023), Global-Digital-Compact_background-note.pdf.

See Eur. Ct. H.R., GLUKHIN v. RUSSIA, App. No. 11519/20 (July 4, 2023), paras. 64-91 (in which the European Court of Human Rights found violations to the rights to privacy and freedom of expression protected by the European Convention on Human Rights with the use of facial-recognition technology against a protester in Moscow).
Advancing Accountability in Cyberspace,
Stimson Center
7. The EU’s General Data Protection Regulation

Reece Iriye

Introduction

Consumer data collection has skyrocketed in the past decade, enabling companies to enhance their products through targeted advertising and personalized services. This increase in sensitive data processing has provided valuable insights for product innovation and user experience optimization, but it also has raised concerns about the invasion of privacy. European Union (EU) citizens and regulators have responded by establishing the strongest and most impactful legal framework enforcing data protection standards to date, the General Data Protection Regulation (GDPR).

DECONSTRUCTING THE MECHANISM

The GDPR outlines a series of guidelines for organizations that process data belonging to individuals located in the EU. Organizations stationed inside and outside the EU are also subject to GDPR guidelines if they collect or process personal data belonging to any individual located in the EU, regardless of their nationality or residence.

These standards are designed to provide individuals in the EU with greater control over their personal data by holding organizations accountable for the ways in which they process individuals’ data. Some key provisions of the GDPR include requirements for organizations to obtain explicit consent from individuals located in the EU to process their data only for indicated purposes; allow individuals to request their personal data to be deleted from the organization’s records; and notify individuals and relevant authorities within 72 hours in the event of data breaches that put consumers’ personal data at risk.

Each member state of the EU appoints their own Data Protection Authority (DPA) with the power to investigate GDPR infringements, interact with organizations to resolve noncompliance, and impose fines for violations. Provisions for DPA appointments grant each member state the autonomy to choose their DPA through a transparent process led by their parliament, government, head of state, or an independent body defined by national legislation.

Member states have the option to nominate a singular person as the DPA for their state, or to designate a committee for data protection with a principal supervisor. For example, Ireland’s Data Protection Commission (DPC) and France’s Commission Nationale de l’Informatique et des Libertés (CNIL) both serve as committees, whereas Austria and Bulgaria employ individual DPAs for GDPR enforcement.
Ireland’s DPC is large and is the primary authority enforcing GDPR provisions against violations by several major U.S. technology companies. The GDPR entrusts DPAs with the authority to address complaints from data subjects or representative bodies/organizations and to conduct investigations, which may be initiated into GDPR compliance.

DPAs have the capacity to impose financial sanctions on companies they declare are violators of GDPR guidelines. Organizations that violate the GDPR can receive penalties that amount to 4% of their global annual revenue or €20 million—whichever value is greater. In addition, the GDPR provides a “one-stop-shop mechanism,” which centralizes decision-making for cross-border cases to a single lead DPA based where a company is legally established.

The GDPR has issued over 2,100 fines as of December 2023, surpassing €4.4 billion in total. The five largest fines amount to nearly two-thirds of the total fines, reflecting the substantial financial repercussions for the most significant breaches of the GDPR. (See Table 1 below.)

<table>
<thead>
<tr>
<th>Company</th>
<th>Fine in Euros (€)</th>
<th>Country</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meta Platforms Ireland Unlimited</td>
<td>€1.2 billion</td>
<td>Ireland</td>
<td>2023</td>
</tr>
<tr>
<td>Amazon Europe Core S.á.r.l.</td>
<td>€746 million</td>
<td>Luxembourg</td>
<td>2021</td>
</tr>
<tr>
<td>Meta Platforms, Inc.</td>
<td>€405 million</td>
<td>Ireland</td>
<td>2022</td>
</tr>
<tr>
<td>Meta Platforms Ireland Limited</td>
<td>€390 million</td>
<td>Ireland</td>
<td>2023</td>
</tr>
<tr>
<td>TikTok Limited</td>
<td>€345 million</td>
<td>Ireland</td>
<td>2023</td>
</tr>
<tr>
<td>Meta Platforms Ireland Limited</td>
<td>€265 million</td>
<td>Ireland</td>
<td>2022</td>
</tr>
<tr>
<td>WhatsApp Ireland Ltd.</td>
<td>€225 million</td>
<td>Ireland</td>
<td>2021</td>
</tr>
<tr>
<td>Google LLC</td>
<td>€90 million</td>
<td>France</td>
<td>2021</td>
</tr>
<tr>
<td>Facebook Ireland Ltd.</td>
<td>€60 million</td>
<td>France</td>
<td>2021</td>
</tr>
<tr>
<td>Google Ireland Ltd.</td>
<td>€60 million</td>
<td>France</td>
<td>2021</td>
</tr>
</tbody>
</table>

Table 1: Summary of Top 10 GDPR Fines in descending order (highest to lowest amount) as of December 23, 2023

The data in Table 1 demonstrates a significant trend: larger GDPR fines are predominantly levied against major technology companies. Large fines against these companies showcase how size and market influence do not exempt them from the reach of GDPR enforcement.

Meta and its subsidiaries, for example, received six of the 10 largest GDPR fines to date as of December 2023 according to Table 1. In Meta’s case, and similarly with many major technology companies, their revenue model relies heavily on ad targeting and content recommendation algorithms driven by users’ personal data. Fines levied towards major technology companies featured in Table 1 generally serve as operational expenses rather than influential steps towards changing how they process personal data due to their multi-billion-dollar valuations.

GDPR fines can be burdensome for newer, smaller businesses that lack the resources of their larger counterparts and are not the focus of media attention for data misuse. Former EU Commissioner of Justice
Viviane Reding, who first proposed the GDPR in 2012 and was a chief architect in its development, identified the disproportionate effects that fines have towards smaller companies in an interview in May 2021:

*For a regulator, it’s easier to control the local football club than a worldwide company. We should leave the local football club alone and focus on the real troublemakers... The enforcement against systematic stealing of data for commercial or political purposes is somehow not so strong.*

Despite the GDPR’s intention to centralize enforcement in the one-stop-shop mechanism, in practice it leaves Ireland and Luxembourg DPAs responsible for holding most Silicon Valley tech giants accountable.

Ireland has particularly been criticized for its leniency in handling GDPR violations. In Ireland, 87% of cross-border GDPR complaints involve major technology companies. The Irish DPC resolved 46 out of 55 of their cross-border complaints from 2018 to 2022 through “amicable resolutions.” This approach involves holding conversations with the organizations in question and proposing mutually agreeable solutions at the discretion of the Irish DPC. Most of Ireland’s cross-border complaints involve repeat offenders, highlighting how the Irish DPC consistently fails to comply with EDPB guidelines. Thus, Ireland’s continuous use of amicable resolutions to resolve GDPR complaints indicate a systemic reluctance to enforce the GDPR with penalties of fines as Reding and other EU policymakers envisioned.

Excluding situations involving amicable resolutions, the EDPB overrules 67% of the rulings made by the Irish DPC. This high degree of intervention by the EDPB in one-stop-shop cases highlights their commitment to firmer GDPR enforcement. However, penalties administered by the EU remain modest. Of the 160 one-stop-shop cases evaluated by the EDPB, only 29 have resulted in fines, and a significant 63% of cases were merely concluded with reprimands from the enforcing body. This minimal enforcement in practice of the GDPR suggests that even the EDPB’s oversight does not always translate into punitive action. Stronger cross-border enforcement mechanisms have been proposed, and some are being implemented to better coordinate enforcement actions.

Nevertheless, the GDPR has still had a noticeable impact on how organizations process personal data across the world. A significant portion of its international influence can be attributed to the “Brussels Effect,” named after the capital of Belgium where the EU’s main institutions are located. The Brussels Effect refers to the EU’s *de facto* regulation of companies who operate across multiple global markets by establishing policies that affect actors who conduct business in the EU but are stationed elsewhere. The EU’s influence is considerable, given it consists of 27 member states, making it influential in the global economy.

Businesses worldwide that leverage consumer data must follow GDPR guidelines if they want to operate in the EU without reprimands. As a result, even countries outside the EU (e.g., Japan, Brazil, India, and the U.K.) have introduced and/or updated their data protection legislation to mirror that of the GDPR. The U.K., for example, applied their version of the GDPR to fine TikTok Technology Unlimited in September 2023 for unlawfully processing the data of 1.4 million children under the age of 13. While the United States has yet to adopt national data protection legislation like the GDPR as of December 2023, several U.S. states (California, Colorado, Connecticut, Utah, Virginia) have implemented laws that mirror aspects of the GDPR. Due to the saturation of the EU market and the establishment of similar laws worldwide, countries and companies beyond the EU’s jurisdiction have found it necessary to adapt to GDPR standards, showcasing the legislation’s role as a *de facto* global standard for data protection.
Context

The GDPR was enacted in 2016 in place of its outdated predecessor, the 1995 Data Protection Directive (DPD). The DPD’s jurisdiction to regulate data processing depends on two important criteria: (1) the organization has an “establishment” in a European Union member state, and (2) the organization conducted processing of EU citizens’ personal data within the context of its regular activities. Pivotal court decisions such as C-230/14 Weltimmo pertaining to the application of national data protection laws and applicable fines drew criticism of the DPD’s vague definition of an “establishment” and highlighted the complexities and gaps within the directive.

The DPD’s enforcement capacity fell short due to its nature as a directive. Unlike EU regulations, which have direct applicability and uniformity across all member states, directives identify goals from the EU that must be met by each individual member state with the freedom to decide how the goals will be met. With these goals set by the DPD, each member state implemented laws with different applications and enforcement procedures, causing disparities in data processing standards across the EU. In 2012, the European Commission—the leading executive body in the EU—recognized the fragmented implementations of data protection laws across EU member states as problematic, which led to a revision cycle on the DPD and eventually the formation of the GDPR.

Both the European Parliament and the Council of the European Union—which are responsible for adopting or rejecting proposed laws—evaluated the European Commission’s proposal during this process, leading to over 4,000 proposed changes. Firms in finance and retail, which handle large amounts of sensitive data and face high compliance costs, largely lobbied against the GDPR. In contrast, many firms, including those from the technology sector, showed overwhelming support for the GDPR, seeking to influence its final shape in their favor.

EU officials eventually decided to halt the ongoing conversations about the GDPR’s implementation. In January 2014, former European Commissioner for Justice Viviane Reding declared that the document was past the revision stage, and the EU would not be stalled in setting the norms for personal data usage. She cited overwhelming concerns about high-profile data breaches and the lack of public trust in data processing by private and public actors as justifications for why the regulation must be implemented:

> There has been a lot of hypocrisy in this debate. For instance, those who called for a high level of data protection in Europe, while simultaneously arguing that the Regulation should be replaced by a Directive. We have listened to these arguments for two years. Round and round in circles while, every day, the headlines have reminded us of why the reform is important. Discussions are mature. The text is ready. It is just a matter of political will.

In March 2014, following Reding’s speech, the progress on reforming EU data protection was affirmed rendered irreversible with a vote from the European Parliament of 621 in favor, 10 against, and 22 abstentions—demonstrating overwhelming support for the regulation. The GDPR was then signed into law in 2016, providing a two-year period for organizations to become GDPR-compliant before becoming enforceable by law in 2018. This timeline highlights the EU’s commitment to setting enforceable standards for people-first data protection laws.
Applicability to Cyber

As the GDPR represents one of the most far-reaching agreements on a data protection issue, understanding its history and impact is important to considering how norms can become standards of behavior. Although the protection this regulation affords affects actors obtaining data in a lawful way, the regulation defines new norms of acceptable behavior for data protection, and its enactment and enforcement provide a norm for the broader world, including states, businesses, and individuals.

The successful establishment of the GDPR stems from a foundation built on shared values regarding data privacy and the institutional authority of the European Parliament. These values are deeply rooted in historical contexts, such as the use of data in the 1930s by Nazi Germany to target Jewish people, and they are enshrined in the EU Charter of Fundamental Rights. The GDPR demonstrates how shared cultural and ethical values and norms can guide the creation of impactful legislation in other areas, such as cybersecurity and cybercrime. In addition, the GDPR showcases how dedication to enacting a policy within a specific region can cause a ripple effect across the world setting global standards for a cyber issue. This global effect of regional policies is continuing to happen in other legislative areas that the EU pursues as part of its broader EU Cybersecurity Strategy.

Key Takeaways and Recommendations

1. Leaders are key drivers of agreements and can leverage common values.

As the GDPR represents one of the most far-reaching agreements on a data protection issue, understanding its history and impact is important to considering how norms can become standards of behavior. Although the protection this regulation affords affects actors obtaining data in a lawful way, the regulation defines new norms of acceptable behavior for data protection, and its enactment and enforcement provide a norm for the broader world, including states, businesses, and individuals.

The successful establishment of the GDPR stems from a foundation built on shared values regarding data privacy and the institutional authority of the European Parliament. These values are deeply rooted in historical contexts, such as the use of data in the 1930s by Nazi Germany to target Jewish people, and they are enshrined in the EU Charter of Fundamental Rights. The GDPR demonstrates how shared cultural and ethical values and norms can guide the creation of impactful legislation in other areas, such as cybersecurity and cybercrime. In addition, the GDPR showcases how dedication to enacting a policy within a specific region can cause a ripple effect across the world setting global standards for a cyber issue. This global effect of regional policies is continuing to happen in other legislative areas that the EU pursues as part of its broader EU Cybersecurity Strategy.

2. Focusing regulation on activities and roles instead of items and technology, while also building in opportunities for review, enables continuous adaptation.

Modifying legal instruments can be a lengthy and tedious process. The GDPR underscores the importance of clear, precise, yet adaptable terminology in regulation. The regulation builds a foundation for clarifying important terms that are fundamental to the framework such as “collecting,” “processing,” and “data
controllers,” and outlines clear guidelines for actors’ roles and responsibilities. This precise identification of individuals and actions establishes clarity, including those who will be investigated for GDPR infringements.

The need for more significant adaptation and iterative review cycles since 2018 when the GDPR was established has become apparent. The realities of the market, including its evolution, must be acknowledged. The EU is thus adapting with some new initiatives, including on enforcement as noted below.42

3. Centralized, uniform, and meaningful enforcement measures are crucial for managing major violations.

The transition from directive to regulation—with the DPD evolving into the GDPR—highlights the need for some uniformity in application. The transition also demonstrates how transformative regulatory policy can be, especially in the cyber domain where borders are not well defined. Policies can have far greater impact when multiple institutions operate under a single law and when penalties are structured for impact, such as fines based on company revenues. A uniform approach simplifies the regulatory landscape for companies operating in multiple countries and enhances the credibility and authority of the enforcement process. However, the effectiveness of state enforcement facilitated by the one-stop-shop mechanism depends on collaboration and uniformity among nations in handling cases related to cross-border processing of personal data. Both the European Parliament and civil society organizations have frequently complained about the inconsistencies and inefficiencies arising from individual countries adhering to their own national procedural regulations, including the potential for forum shopping.43 Thus, the EU has proposed a new process for even more centralized GDPR enforcement in recognition of the difficulties in cross-border enforcement and the growing threats from cyber and AI, while actively developing agreement on common EU security standards and vulnerability protections.44 The EU’s upcoming procedural regulation, slated for consideration by Parliament in April 2024, aims to standardize and harmonize states’ disparate approaches.45 Likewise, international cybersecurity norms/laws would benefit from a more systematized mechanism to facilitate cross-border cooperation among states, organizations, and experts to more effectively address cyber threats.

4. Supranational organizations like the EU (and like-minded states) are key change-makers and can leverage their global influence.

Regional frameworks and like-minded states working together may offer more value than global approaches when agreement on shared values and institutions exists. As demonstrated by the Brussels Effect, the EU’s influence in the global economy positions supranational organizations as pivotal changemakers in the realm of cyber regulation. The EU’s considerable size and market power grant it the capability to set global standards as many companies outside Europe find it necessary to comply with GDPR guidelines to maintain access to the EU market. The EU’s influence in the cyber domain highlights the significant role that supranational organizations and like-minded states can play in shaping global digital policies, particularly in areas where private actors frequently operate and cross-border interactions regularly occur.
The significant strides made by the EU’s progress in defining its digital future may well inspire others to consider similar approaches. As the EU builds out operational aspects of its forthcoming Cyber Solidarity Act that includes a Cybersecurity Incident Review Mechanism, the EU should consider how adaptation of its information-sharing mechanism, including standardized documentation and review procedures for incidents, might be developed for use by other entities. The opportunity for consistent international reporting frameworks would help with international data collection, risk assessment/management, and support of norms, international law, and accountability. Integration into the broader EU Cyber Diplomacy Toolbox and into other efforts would be beneficial for better defining efforts that could involve other stakeholders in technical and political attribution and accountability.

The larger Council of Europe, with 46 member states, successfully ratified the Budapest Convention on Cybercrime in 2004. The principles of the Convention drew many like-minded states to be parties. In contrast, the UN’s recently proposed international treaty on cybercrime has stalled primarily over differing values placed on concerns for human rights protections. How broader international agreements can develop via the work of regional organizations and like-minded states is also evidenced by the Council of Europe’s successful recent work in developing a framework convention on artificial intelligence and then sharing its work, including its risks and impact assessments, through the Organization for Security and Cooperation in Europe and with the African Union.

The UN Secretary-General has suggested the need for a new mechanism for attribution to hold states to account, while the Organization for Economic Coordination and Development (OECD) in its research also noted the need for a new attribution mechanism to address cybercrime. Frameworks for technical, legal, and political attribution have been suggested as states are asking for more guidance. A regional organization could well take the lead on working with stakeholders on developing an agreed framework for attribution that would promote accountability and support agreed norms and international laws.
Endnotes


2 Ben Wolford, “What is GDPR, the EU’s new data protection law?”, https://gdpr.eu/what-is-gdpr/, GDPR.eu is cofunded by the Horizon 2020 Framework Programme of the European Union and operated by Proton AG, 2024.


4 The GDPR. Articles 51-59.

5 The GDPR. Articles 51-59.

6 “Our Members | European Data Protection Board.” European Data Protection Board, 8 Nov. 2023, edpb.europa.eu/about-edpb/about-edpb/members_en#:~:text=Austria%0A%0A%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%23%2�


This is also true in other EU initiatives, e.g., Kelvin Chan and The Associated Press, “Tech’s 6 ‘gatekeepers’—including Amazon, Apple, Meta and Microsoft—are about to face heavy new scrutiny as Europe aims for ‘fairer’ digital markets,” https://fortune.com/europe/2024/03/06/tech-6-gatekeepers-amazon-apple-meta-google-tiktok-microsoft-dma-europe-fairer-digital-markets/, Fortune, March 6 2024; Jay Peters, “How the EU’s DMA is changing Big Tech: all of the news and updates,” https://www.theverge.com/24040543/eu-dma-digital-markets-act-big-tech-antitrust, The Verge, May 14 2024.


As the European Union Agency for Cybersecurity (ENISA) promotes best practices in terms of linking the tactical, operational, and strategic levels and appropriate information sharing (https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management), the EU's Diplomatic Toolbox (See Section 4.21 on sharing with stakeholders and Section 5 on attribution) and Foreign Information Manipulation and Interference Toolbox (https://www.eas.europa.eu/eais/tackling-disinformation-foreign-information-manipulation-interference_en#45330), European Union External Action has already outlined some types of and ways that incident information could be shared and could be better systematized. See also: Erica Moret and Patryk Pawlak, “The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?”, https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/EUISS-Brief_24_Cyber_sanctions.pdf, EU Institute for Security Studies (EUISS), July 2017.


8. Private Actors, State Responsibility

James Siebens and Anne-Marie Buzatu

Defining State Responsibility for PMSCs

In 2008, “The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies (PMSCs) during armed conflict” (hereafter the Montreux Document) was adopted. It was the fruit of collaborative efforts by Switzerland and the International Committee of the Red Cross (ICRC), following years of expert dialogue, multi-stakeholder consultations, and international negotiations. The resulting document identified pertinent existing legal obligations for states under international humanitarian law (IHL), or the law of armed conflict, vis-à-vis PMSCs and established human rights respecting practices for states to hire and employ private security companies in accordance with international law. It has since gained the support and participation of 59 states, including the United States (U.S.), France, the United Kingdom (U.K.), and China, as well as organizations like the North Atlantic Treaty Organization (NATO) and the European Union (EU).

While the Montreux Document is a normative instrument, rather than a legally binding treaty, the Document reaffirms the legal obligations of states under existing international law and restates those that are pertinent with regards to PMSCs. As such, it seeks to reinforce common understandings around key legal obligations and consider them through the lens of private military and security actors that operate within the context of an armed conflict. “It addresses substantive legal concerns, such as the status of PMSC personnel under the 1949 Geneva Conventions, individual accountability for misconduct in different jurisdictions, and the authorities’ duty to oversee and screen the actions of firms for potential misconduct.”

In so doing, the document articulates that state responsibility for the actions of PMSCs lies with their countries of residence, the governments that contract them, and the governments on whose territory they are operating. By endorsing the Montreux Document, states effectively publicly confirm that they understand their existing legal obligations under the Geneva Conventions to be interpreted in the same manner as they are restated in the Montreux Document.

The Montreux Document is a groundbreaking document, and one that is particularly relevant for the current geopolitical situation in which broad agreement on international conventions has proven elusive. It represents an alternative approach to launching a lengthy process to develop a new convention on PMSCs, which would likely lack the support of states that would be important for its implementation, and furthermore might weaken existing international obligations. The Montreux Document provides an example of updating existing legal obligations to respond to new challenges without a drawn-out and politically risky or difficult process.
A cautionary counterexample is the International Convention against the Recruitment, Use, Financing, and Training of Mercenaries, commonly known as the UN Mercenary Convention. Negotiations for the Convention began in the late 1970s led by Nigeria, following concerns about the impact of mercenaries in armed conflicts particularly in Africa. After nearly two decades of negotiations and several sessions, marked by complexities and delays, the Convention was adopted on December 4, 1989, and only entered into force on October 20, 2001, after securing the necessary ratifications. Currently, the treaty has been ratified by 37 states, with enforcement of treaty being little to non-existent.\(^5\)

**Industry-led Accountability**

The development of the International Code of Conduct for Private Security Service Providers (ICoC, or “the Code”) involved private actors, including security companies, and civil society actors to a greater degree than the Montreux Document. Mindful that the Montreux Document applies to states, and not directly to PMSCs themselves, the private security industry called on Switzerland to develop a mechanism that would hold them directly accountable. In response, the Swiss initiative to develop the ICoC began in January 2009, culminating in its finalization and adoption in November of 2010. The ICoC contains 70 provisions for private security companies grounded in international human rights law regarding the conduct of private security personnel, including standards for use of force and detention of persons as well as prohibitions of certain behaviors such as carrying out torture or gender-based violence. It also contains specific commitments by affiliated companies regarding management and governance of the private security company.

While the ICoC initially gained broad support from the private security industry, with more than 700 companies signing the document, it lacked any enforcement mechanism to oversee companies’ implementation of and adherence to the ICoC. In response, the International Code of Conduct Association (ICoCA) was established in 2013 with the goal of promoting responsible and ethical conduct among PMSCs. ICoCA is a multi-stakeholder initiative involving governments, PMSCs, civil society organizations, and other stakeholders working to encourage PMSCs to adhere to the common set of standards and principles, outlined in the ICoC.

The preamble of the ICoC not only references and endorses the principles of the Montreux Document but also sets forth a series of obligations for Member and Affiliate Companies. These companies are mandated to operate in strict compliance with both national and international laws and regulations, as well as to adhere to established corporate standards of business conduct. Fundamental to these obligations is the recognition and support of the rule of law, alongside a firm commitment to respecting human rights and safeguarding the interests of their clients. Additionally, the Code emphasizes the importance of establishing and maintaining robust internal governance frameworks.

These governance frameworks are essential for deterring, monitoring, reporting, and addressing any adverse impacts on human rights effectively. Moreover, the Code mandates that these companies provide mechanisms for addressing and resolving any allegations of activities that contravene applicable laws or the Code’s standards. This includes cooperation in good faith with both national and international authorities, particularly concerning investigations into violations of criminal law, international humanitarian law, or human rights abuses. Through these stipulations, the ICoC aims to foster a responsible, accountable, and ethical private security industry.
While the Montreux Document is not a mechanism per se, and therefore is not implemented as such, continued government engagement was supported through the Montreux Document Forum (MDF), which held annual plenary meetings from 2014 until 2021. In addition to the annual plenary, the Montreux Document Forum hosted regular meetings of a Maritime Security Working Group, as well as an ICoCA Working Group. Since that time, the MDF has not held in-person meetings; nonetheless, it has continued to gain new members, with Slovakia joining in 2022 and Romania joining in 2023.

ICoCA, the oversight and governance mechanism for “the Code”, is supported by membership dues, as well as financial contributions by the governments of the U.S., UK, Sweden, and Switzerland. The membership of the ICoCA is made up of private security companies, governments, and civil society organizations, with each stakeholder pillar having an important function for implementing the Code. There are three member categories for private security companies: 1) “Certified” Member Companies, who have obtained approved third party certification that their policies and processes are in accordance with the code; 2) Member Companies, who have not yet obtained third-party certification, but who commit to doing so by December 31st of the third year after they have joined; and 3) Affiliate Companies, who are not seeking third-party certification, but who commit to continuous improvement in terms of implementing the Code. All companies commit to operating in accordance with the Code of Conduct, are subject to monitoring by ICoCA (both desk monitoring and in the field), submit an annual self-assessment, and pay a joining fee and annual dues.

The ICoCA also has a complaints process to receive complaints about ICoCA members and affiliate companies. Complaints may be submitted by anybody who has been harmed or has reason to believe that a violation of the Code occurred or is about to occur. The complaints process is overseen by a complaints committee, made up of Board Members from all three stakeholder pillars. For complaints alleging criminal activity, due diligence is conducted to determine jurisdiction, and the matter may be reported to competent authorities. These complaints are not processed further until after review and decision by the Board.

To complement ICoCA’s oversight, several governments and companies have either enacted laws or policies that require membership in ICoCA of certain private security companies they contract with. This “coregulation” further hardens the soft human-rights protecting regulation through contractual requirements and financial incentives: in order to obtain and/or keep contracts, companies must comply with the requirements of the ICoC/A.

For example, in its “Private Security Services Abroad” laws of 2015 and 2020, Switzerland requires mandatory reporting and ICoCA membership for certain private security services provided abroad in “complex environments.” This is actively overseen by its Export Controls and Private Security Services Section. The UN and other governments, including Australia, Canada, U.S., and the UK have adopted policies that require ICoCA membership in good standing for private security contractors providing particular services. Finally, some private clients have also introduced IcoC/A adherence in the contracts of their private security companies.

This “mosaic” approach of reinforcing multistakeholder governance through national laws and contracting policies that reaffirm the same standards helps to fill in the governance gaps of traditional regulatory frameworks and give more teeth to cross-border oversight and accountability, improving governance effectiveness and reducing impunity.
In addition to its certification, monitoring, and complaints functions, ICoCA provides guidance to its members and affiliates through advisory services and capacity-building. For example, the ICoCA provides tailored feedback to its member and affiliate companies on the companies’ annual reports of their compliance with the code and helps them develop workplans that focus on areas that need to improve. It has also developed guidance documents on developing and operating fair and accessible company grievance mechanisms that offer effective remedies, as well as on preventing and addressing sexual exploitation and abuse. The ICoCA conducts research, with two projects currently looking at workplace conditions of private security companies, as well as the use of advanced technologies in the private security sector. Finally, the ICoCA offers capacity-building courses “to build the capacity and ability [of Member and Affiliate Companies] to fully meet the international human rights and humanitarian law principles articulated in the International Code of Conduct.”

The Montreux Document has the support and participation of 59 states, including China, France, U.K., and the U.S. as well as organizations like NATO and the EU. Despite the lack of a formal implementation mechanism, there is evidence suggesting the Montreux Document is having a positive impact on the ground. Independent research conducted by Charlotte Penel and Ulrich Petersohn presents compelling evidence that the implementation of the Montreux Document has contributed to a decrease in violence against civilians during and after hostilities.

ICoCA membership includes seven governments (Australia, Canada, Norway, Sweden, Switzerland, U.K., and the U.S.), as well as 142 private security companies, 55 civil society organizations, and 75 “observers” (often private researchers or insurance companies). Since 2015, 33 complaints have been filed against ICoCA member companies, with six companies found to have committed violations. According to the ICoCA website, 22 incidents and 22 complaints have been reported in the last 12 months. This would seem to indicate an increase in awareness and use of the complaints function.

From the beginning, private security companies, civil society organizations and governments were involved in the ICoC process, and the decision-making process required buy-in from all stakeholder
groups. While both the development of the ICoC and the ICoCA strove to take decisions by consensus, in the (very rare) case that consensus could not be achieved, significant support from each stakeholder group was required for a decision to be taken. For example, the ICoCA governance framework was composed of 12 members, four from each stakeholder group. In order for a decision to be approved, this required a minimum of eight votes, with a minimum of two from each stakeholder group. This decision-making formulation, with the possibility of a vote, drove consensus, and encouraged discussions that led to innovative and ultimately effective decisions. Clients of private security companies and subject-matter experts/academics were also included in discussions, particularly in the development of the ICoC, but were not part of the stakeholder pillar voting framework.  

**Key Takeaways and Recommendations**

The successful implementation of the UN Framework for Responsible Behavior in Cyberspace can be significantly enhanced by adopting a model akin to the Montreux Document and ICoCA. This approach would necessitate a multi-stakeholder forum, fostering a collaborative environment for states, private sector entities, civil society, and international organizations. Clients, academics, and other subject-matter experts could also provide useful contributions. Such a platform would not only encourage dialogue but also facilitate the sharing of best practices and experiences. Drawing inspiration from the International Code of Conduct for Private Security Service Providers, a specialized code of conduct tailored for cyberspace actors could be developed. This code would outline responsible behavior and practices in line with international norms, emphasizing the need for a human rights-centric approach in the digital age. Regular review and adaptation of these norms would ensure their relevance in the face of evolving cyber threats and technological advancements.

Accountability and transparency are pivotal in the realm of cyberspace governance, much as they are in the regulation of private military and security companies. Robust mechanisms to monitor adherence to these norms, similar to the third-party audits and assessments used for private security companies under the ICoCA, would be instrumental. For instance, in cases of information communication technology (ICT) incidents, two of the voluntary and non-binding norms for responsible state behavior in the use of ICTs that have been adopted by the UN would benefit from these suggested accountability practices. Norms 13 (b) and 13 (h) encourage states to actively participate in information exchange and mutual assistance, in a process organized by a centralized platform with a multistakeholder oversight framework. Moreover, the implementation of the norm that calls to ensure the integrity of the ICT supply chain (which also relates to Norm 13 (i)) and the non-harming of other states’ emergency response teams (Norm 13 (k)) would greatly benefit from enhanced international cooperation and accountability measures that could be provided under such a platform.

Operationalization of the 11 norms for Responsible State Behavior in Cyberspace would be bolstered through a collaborative and multi-faceted, multistakeholder approach, underpinned by the principles of accountability, international cooperation, and human rights. The Montreux Document and ICoCA can serve as inspiration, demonstrating the effectiveness of meaningful multistakeholder engagement and the adoption of a code of conduct in addressing complex security issues. By drawing on these models, the implementation of the norms can be strengthened, ensuring a more secure, stable, and responsible cyberspace for all actors involved.
Endnotes


4 This is a concern voiced by legal experts and civil society organizations, such as ICT4Peace Foundation.


11 Buzatu, Towards an international Code of Conduct, 60-63.

12 Buzatu, Towards an international Code of Conduct, 45-63.


9. Can the African Peer Review Mechanism Effectively Govern Cybersecurity and Accountability?

Molichi Makumane

What is the African Peer Review Mechanism?

The African Peer Review Mechanism (APRM) has served as a regional peer review mechanism since 2003 under the African Union (AU) to oversee monitoring and evaluation in all key governance areas of the continent. It enables its 42 participating states to conform to agreed values, codes, and standards that lead to political stability, high economic growth, and sustainable development, as well as accelerated subregional and continental economic integration. Member states share their experiences and best practices, including identifying deficiencies and assessing the needs for capacity building. AU member states have taken pride in their distinctive regional peer review mechanism, from developing a self-assessment tool and process to evaluate African governance strengths and weaknesses, to attaining membership by more than half of the AU’s countries. As a result, economic opportunities and human development indicators of good governance improved between 2012-2021, according to the Ibrahim Index of African Governance. Nine out of the top 10 countries showing governance improvement in the Index are APRM member states, which speaks to the impact of the organization.

As recently as 2017, positive signs of governance initiatives were becoming apparent and the APRM was given an expanded dual mandate of monitoring and evaluating the AU’s Agenda 2063 as well as progress toward achievement of the Sustainable Development Goals by 2030. The APRM now plays a more prominent role in defining the governance framework landscape in democratic, political, economic, and management processes, as well as in socioeconomic and corporate areas. In 2023, the APRM celebrated 20 years under the theme “Accelerating and Deepening Governance Reform, Measures, and Intervention.”

The success of the APRM is particularly interesting in the context of Africa’s subregions that are composed of developing countries; such countries have governance deficits and leaders that might be unwilling or unable to change their country’s political systems in response to global good governance efforts. Numerous conditions, such as enhanced coordination, monitoring of assessments in a more timely manner, make regional peer review mechanisms rather than continent-wide ones attractive. Nonetheless, the APRM offers significant benefits, which compels many states and partners to use a broader lens in supporting regional initiatives. A reading of the APRM Legacy Report organized by South African President Cyril Ramaphosa, the 2020-2022 APRM Chair, identified several pillars that contribute to the APRM’s success. Two are particularly relevant for this chapter: 1) Assistance to member states with governance monitoring and evaluation (M&E) activities; and 2) providing APRM tools, such as the African Union Governance Atlas. Certain aspects of these two pillars interact with one another to create a virtuous cycle.
Governance M&E: A well-crafted national programme of action (NPoA) provides critical information for the government as well as nongovernmental stakeholders to remedy the challenges identified during the baseline review and identify legislative, capacity, or resourcing gaps alongside the necessary resources to address them. In its original conception, the NPoAs could be used by investors and partners when making investment decisions, especially in areas of weak governance. The findings and NPoA could be used as governance assessments. The APRM has convened capacity-building workshops on the integration of APRM national programs of action into national development plans.

APRM Tools: The fact that the APRM is already undertaking several types of country reviews creates a hub of governance indicators and indices on the continent. For example, in 2019, APRM’s members decided to create an African Union Governance Atlas to communicate to policymakers and the public data on aspects such as elections, the rule of law, the delivery of public goods, access to information, judicial and legislative independence, economic governance, corruption, and civil society participation. In 2020, the APRM completed profiles of all 55 AU countries for the Governance Atlas. Once produced, the atlas will serve as a platform for investors and partners to engage with African states in several ways. First, it will provide background information for investors and partners, who often require governance assessments before making investment decisions. Second, it will highlight demonstrable progress across governance indicators and capabilities, which can be highly advantageous.

Assessments and Oversight: Notably, the APRM has several layers of institutional oversight, including the APRM Forum, the Committee of Focal Points, and the Panel of Eminent Persons. The forum participants are heads of states, as well as leaders of all APRM member states, who serve a two-year tenure and produce and review reports. The committee is composed of focal point representatives from participating states and tasked with, among other responsibilities, oversight over the budget and the professionalism and accountability of the Secretariat. The first seven-member member panel of eminent persons, appointed in 2003, comprised distinguished Africans from participating states with integrity, impartiality, and moral stature—qualities needed to oversee “governance and performance of the Country Review Process as well as other processes that need partnerships and to safeguard African ownership of the Country Review Process.”

Drawbacks and Limitations

Distinct factors create a compelling advantage for the APRM for internal and external parties (mainly international organizations), including improvement in the quality of governance, deepening of democracy and national institutions, and the cultivation of national consensus and political trust. Yet other factors hold the APRM back from reaching its full potential. AU member states still have a way to go in terms of fully supporting the APRM, due to funding constraints. Of the 42 participating states, 25 have had a baseline review since 2006. Fewer than 10 have conducted their second-generation peer reviews (subsequent reviews to monitor progress against the programme of action and shared objectives identified in first review) owing to lack of funds and an overstretched Secretariat. This could be a major missed opportunity. Increasing the share of countries that undertake second-generation reviews has the potential to fuel significant, measurable improvements in positive governance.

The APRM strategic plan report highlighted the need for a financially sustainable and credible Secretariat. For example, the APRM Trust Fund, established and managed by the UN Development Programme (UNDP), has run dry due to non-payment of membership contributions. Funds were mostly
from contributions by participating African countries, with each country expected to contribute USD $100 000 per year. The Development Bank of Southern Africa maintained an account on behalf of the APRM. When the APRM was incorporated as an AU organ, the assembly decided “to integrate the APRM budget in the statutory Union budget funded by Member States.” Resource mobilization remains a priority for the APRM.

Different Paths to Scale

Intergovernmental peer review mechanisms take varied paths to success, but they share certain common elements, especially on specific concerns of states, such as accountability and transparency. A special area of potential is digital governance and global cooperation as outlined by the APRM at the 18th Annual Internet Governance Forum in 2023. The APRM can share key lessons on African governance in different domains to enhance and optimize the use of technology in key governance areas such as elections, citizen engagement, access to information, and technology security.

The APRM has four types of reviews: 1) a review specifically for State parties undertaken 18 months after signing the declaration to provide a national action plan to adhere to the declaration; 2) a review requested by a state party for its own reasons; 3) periodic reviews every two-to-four years; 4) an early signs review that are topic specific reports that cover a theme or sector of interest for governance in African states. Based on the analysis of the APRM’s distinct elements, the author of this paper recommends the following three strategies to promote accountability and transparency in international cyber and international communication technology (ICT) security governance.

1. **Post-accession review:** Peer review mechanisms establish post-accession reviews to identify gaps and opportunities after a state has acceded to or joined an instrument. The use of this type of review for ICT security is intended to generate significant insights pertaining to how civil society groups and governments interact. Civil society organizations can participate in this type of review at different levels: in the national governing council, which sets the rules and plans for the review at the national level and supervises the research, consultation, writing and editing of the Country Self-Assessment Report; through a panel, which supervises the peer review system as a whole and guides individual country assessments; and last, by participating in the country review teams, which are interdisciplinary teams of experts from academia and business who visit each country and write the final assessment and recommendations. For example, a cyber-related review mission could assess accountability and transparency, including obtaining clarity from states on operating standards, principles, and what constitutes responsible behavior; how states prioritize cybersecurity investments and measure dividends; and how they collaborate to call out malicious behavior.

2. **Reviews requested by a state party for their own reasons:** In the realm of ICT security, the willingness of countries to submit to constructive criticism by their peers on issues linked to such areas as public safety online would testify to the value that countries attach to guaranteeing a safe online environment for their populations. Although a cyber treaty does not exist, to mandate such reviews, existing governance bodies, including at the UN, could explore how to approach or manage a peer review request process. The UN could, for instance, consider to what extent states are pursuing some of the positive commitments contained in the 11 voluntary norms for...
responsible state behavior in cyberspace, endorsed by the UN General Assembly. The review could also be focused on assessing the effectiveness of the existing national and local mechanisms developed to prevent and manage selected thematic areas or in meeting recommendations set out by the UN Open-ended Working Group (OEWG) on ICTs.

3. **Early signs review:** This kind of review could be initiated to identify the challenges related to, for instance, the role of ICT in future conflicts. The focus of such an effort could be to review the experiences of countries that have encountered problems pertaining to ICT during conflicts and consolidate the findings. An early signs review could also make recommendations in accordance with international law on the promotion of human rights and fundamental freedoms and help to establish a relationship between peace and security on the one hand and ICT security governance on the other. It could also explore the nexus between governance and development and the role of regional organizations and UN agencies in international ICT security governance. The APRM has conducted reviews on unconstitutional changes of government (UCGs) with recommendations on how AU member states can invest efforts toward preventing, managing, and responding to UCGs with the ultimate objective of promoting peace, security, and stability.

### What Happens Now?

Despite some concerns about the global accountability and transparency in the international cybersecurity realm, there is ample reason to be optimistic about the potential for peer review mechanisms — either developing new ones specifically for cyber issues or integrating cyber and digital security into existing peer review mechanisms.

From a leadership perspective, meeting the twin challenge of capacities and capabilities while developing harmony between traditional peer review themes and cyber activities will require a new approach. Establishing a relationship between regional peer review mechanisms and the OEWG, or a future UN intergovernmental body, will be crucial. The latter can encourage states to be transparent regarding their activities in peer review self-assessments. Likewise, in a new mechanism with oversight from a UN intergovernmental body, leveraging the UN Secretariat and adding an oversight role to the chairperson's responsibilities will be critical for states to hold each other accountable in implementing the rules, norms, and principles of responsible state behavior. Moreover, states will be well positioned to promote a common understanding of threats to information security and to work cooperatively to prevent and counter such threats, as well as others.

In addition to the advantages of the peer review process, such as providing governance assessments for external partners and investors, there are other reasons for optimism. The process helps to foster the political will for an improvement in cyber governance. The experience of the APRM has demonstrated that many African governments are willing to participate in such review processes. As with accountability measures, a crucial key to success is ambition. In the current geopolitical environment, several areas of international cyber governance, both voluntary and binding, have the potential to be pursued. Such efforts can promote bold ambitions while encouraging the adoption of context-specific intergovernmental peer reviews and increasing cyber resilience.
The author of this chapter makes the following recommendations:

1. Establish a consolidated international ICT security plan to create a conducive political, economic, legal and social environment in countries to achieve agreed-upon levels of cybersecurity maturity and foster support for enforcement mechanisms.

2. Engage with relevant UN agencies and other entities on annual progress reports to the UN Open-ended Working Group and implementation measures and foster international support for funding.

3. Develop an intergovernmental peer review mechanism, to ensure that progress on norms, rules, and principles of responsible state behavior, international law, confidence-building measures, and sound international security practices highlighted in the ICT security plan become irreversible.20

4. Include the envisaged peer review mechanism in regional governance and oversight structures.
Endnotes

1 The African Union is comprised of 55 Member States, 42 of which participate in the APRM.


6 Carnegie Endowment, Aiding Governance, 44.


16 APRM, APRM at IGF 2023.


10. Market Incentives

Debra Decker

Security threats posed by the internet, artificial intelligence (AI), and quantum computing are multiplying at a speed with which governments and legislatures cannot possibly keep pace. Currently, market mechanisms such as credit ratings, product and service security ratings, liability adjustments, procurement requirements, tax adjustments, grants, and insurance are relatively untapped incentives that can play a pivotal role in promoting accountability for securing cyberspace. Market incentives to promote cybersecurity would help build a case that shifts security from a burdensome requirement or regulation to a value-added effort. Broadly speaking, market mechanisms are in different stages—some require more capacity or development, while others are evolving on their own terms.

One market incentive that could benefit from more coordinated support and integration into policy discussions is insurance. The industry’s effect on cybersecurity is not fully appreciated, and the accountability required of the insured and of the insurance industry is not yet well leveraged.

Although much has already been written about cyber insurance in relation to cyber issues within international relations, this case study considers cyber accountability from multiple perspectives to consider how collaborative public-private approaches can leverage commercial insurance to help better manage global cyber risks. Insurance is a mechanism the insureds use to transfer and share risks they do not want to carry themselves. Insurers hold the insured to account for certain behaviors as a condition of coverage and price their premiums based partly on the underwriters’ assessments of risks. Insurers are likewise held to account for their performance in cyberspace by their owners who provide the capital, by governments, and by the public who consider the societal effects of insurers’ actions, such as their role in ransomware claims.1 Government regulations, liability considerations, and broader enterprise risk concerns within the insurance ecosystem all affect the industry and can be leveraged to improve cybersecurity.

Insurance as a Mechanism for Developing and Enforcing Norms for Commercial Coverage

Property and casualty insurance are the two main classes of commercial insurance.2 Property insurance covers business losses ranging from natural hazards to criminal acts, with losses relating not just to the property itself but also to losses from disruptions in business continuity.3 Casualty insurance covers losses related to an individual’s or business’s legal liability, such as others’ losses from business products, operations, or property. Outside of these larger classes of insurance exist specialty insurance policies, such
as professional liability and errors and omissions (E&O) to cover claims against a company for negligent performance. Cyber insurance is found within this class of specialty insurance. Many property and casualty policies have been “silent” on cyber risks, making it unclear what was covered. To address this problem, a special class of cyber insurance policies has been developed as a carve-out from other policies.

Cyber insurance is intended to indemnify organizations for expenses and financial losses associated with “security incidents” and “privacy events,” as defined in the terms of the policies. A vast amount of coverage types is potentially available under most cyber insurance policies, such as for business continuity, but some cyber risks may not be addressed via a cyber policy. The associated risks typically not covered under cyber policies would be for losses such as general property damage, bodily injury, product recall, environmental impacts, etc. Cyber insurance is not yet as uniform as other property and casualty insurance, so businesses rely on the expertise of specialized cyber insurance brokers to determine the most appropriate policies and terms for their needs. The cyber insurance market is the fastest growing area of insurance, with an estimated $12-13 billion in premiums in 2022 but expected to grow annually by 25-30%.

**INSURANCE CAN DRIVE ACCOUNTABILITY FOR INSURED'S GOOD STANDARDS OF PERFORMANCE**

The insurance industry has evolved over the years from when security professionals accompanied underwriters on client sites to help assess security, to clients completing long questionnaire-based cyber assessments, to today’s more streamlined assessments of management controls. Through these assessments, insurance can drive norms of behavior for those insured—but it is complex!

Prospective policyholders now complete an insurance application that typically includes questions regarding network protections, access management such as multifactor authentication, backup solutions, employee awareness, and privacy governance, among other considerations. Marsh, the world’s largest insurance broker, developed an assessment tool based on claims data and extensive client questionnaires to identify a potential insured’s actions that effectively reduce cyber risks. This tool identified key controls, which map to the US NIST Cybersecurity Framework and can define an entity’s cybersecurity “tier” that represents the strength of its risk controls. Other certification and measurement schemes are also taken into account, such as Cybersecurity Capability Maturity Model, ISO 27000 series, European Union (EU) digital requirements, and individual states’ models. In some cases, independent evaluators certify performance. Thus, in applying for cyber coverage, entities represent their performance and attest to their cybersecurity controls, their governance and compliance efforts around data privacy, and certain cyber hygiene behaviors that underwriters, who specialize in risk assessment, evaluate for coverage.

Cyber policy premiums can vary widely, but the inconsistency of coverage terms and conditions across insurers requires the prospective insured to use a decision matrix that includes consideration of premium, coverage terms, retention/deductible levels, and the total limit of coverage — all desired factors to determine the most appropriate cyber insurance program. Given the generally modest insurance policy limits today, larger companies with higher risk exposures typically have to build up their desired cyber coverage using multiple insurers. Other factors often considered when choosing insurance coverage include whether the company has other covers with an insurer, what level of flexibility a company would like around selection of third-party cyber incident vendors (such as forensic specialists and other firms), and the insurer’s domicile (U.S., Great Britain, Bermuda, or other domestic markets for foreign-
domiciled entities). For the insurance company, premium pricing is a function of the deductible levels in the policy, its limits of coverage in dollar terms, and the policy wordings and exclusions. Premiums can vary among insurers for the same entity based on the insurer’s own risk appetite for that industry class, its larger relationship with the insured who may have other coverages with the insurer, the competition in the market from other insurers, and the insurer’s ability to earn investment income on the premiums it sets aside to cover future expected claims.

Not all organizations obtain cyber coverage. Some retain cyber risks. Others may set up captive insurers to manage their risks or establish risk pools with those in their industry, such as via the new MIRIS pool in Europe or in the civil nuclear industry. While some organizations may not see the value of cyber insurance given current policy terms, the insurance industry is evolving to provide new services alongside indemnifying policyholders’ losses and will likely attract more prospective clients to the already growing cyber insurance market. Brokers and insurers are increasingly providing wraparound services to help organizations not only reduce their vulnerability but also prepare for and be resilient to any future cyber incident. For example, Marsh reorganized in 2024 to provide more integrated services, and its brokers can also help explain some of the technical aspects of coverage. New entrants into the market include firms like Microsoft and Amazon that partner with insurers to provide coverage as well as monitoring services, threat information, and risk management advice.

An important aspect of insurers holding policyholders accountable is an entity’s application, as it becomes an attestation of performance. If a policyholder company attests to having certain standards of performance that it does not actually possess, the insurance coverage may be void. The insurance industry recognizes that it needs to better understand what norms work to reduce cyber risks so that it can price policies more accurately, establish more effective norms as requirements of coverage, and help individual insurers better assess their exposure to risks. Swiss Re Institute and the AXA Research Fund, research entities established by two leading re/insurers, are jointly supporting independent research to this end with a focus on resilience to systemic risks, a topic discussed later in this paper.

INSURANCE MAY HELP DRIVE BETTER ACCOUNTABILITY OVER TECH PROVIDERS

Technology providers include providers of hardware, software and managed services, known as managed service providers (MSP). They represent special cases for insurers. Insurers may cover losses arising from claims by other insureds using their products and services and for insurance coverage contracted with these providers/managers for professional indemnity, often in the form of professional liability as well as errors and omissions (E&O) insurance. These technology providers/managers are critical components of the supply chain and pose significant risks across client groups due to their vulnerabilities/ poor performance and thus to insurers, who fear “risk aggregation” and systemic risks such as evidenced in SolarWinds, MS Exchange, and Change Healthcare incidents.

Since it is difficult today to assess the quality of some hardware, software, or MSPs, this challenge means insurers cannot easily consider their quality in their insurance contracts both for their liability coverage and for the cyber coverage of the entities using their tech products/services. Insurance requirements alone could not, in any case, drive better, more secure services from these entities. Tech providers already protect themselves from liability and performance claims through expressed limitations on liabilities in sales agreements, licensing exclusions, and bespoke MSP service agreements. However, there is a trend
Advancing Accountability in Cyberspace, Stimson Center

toward clarity about the responsibilities and prospective liabilities of these tech industries that may
drive more performance claims against tech providers/managers and might drive more of them to insure
for their errors and omissions. In late 2023, a notable class action lawsuit was filed against U.S. tech
company Intel for security issues in its central processing units (CPUs) and its remediation actions that
slowed computer performance. Nonetheless, cautions are needed as insurance itself could become a
moral hazard if risks are not appropriately shared and priced in order to move the tech providers toward
more secure design/performance rather than assumptions of liability coverage for poor security.

The potential for litigation, fines, and reputational harm may increase as governments express heightened
requirements for the IT industry’s performance. U.S. President Biden’s 2023 cybersecurity strategy calls
to “reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software
vulnerabilities, and other risks created by software and digital technologies.” The EU has adopted a
voluntary certification scheme and some mandatory security requirements for hardware and software
products. The World Economic Forum has called for international certification schemes. Industry
security will increase, but users’ security expectations will also rise. Thus, deviations from these regulatory
or best-practice performances that result in user harms may well lead to increased, more substantiated
claims; and insurers will be involved in covering some of the tech providers’ related costs through the
providers’ own professional liability policies. Some NGOs such as Atlantic Council had already been
calling for more explicit standards of care for tech providers so that the judicial system can be leveraged
to reduce risks.

In sum, insurers have an interest in encouraging progress to establish agreed standards of secure
development for software, adopt security by design standards, and promote safe havens from legal liability
for those who abide by best practices to meet cybersecurity standards, like those that the US SAFETY Act
provides to entities that have certified good practices. All of these good practices can increase security
and protect tech providers and thereby insurers of those providers from losses. Once good practices
are identified and become norms, regulations, or laws, insurers can better assess their carried risks and
review and appropriately structure policy conditions based on performance of hardware, software, and
service providers—or can deny coverage.

Issues of tech companies’ liability for security and their insurance coverage have arisen already, including in
2017 with the Wanna Cry exploit, a ransomware cyberworm that infected unpatched Microsoft operating
systems. Insurers’ engagement should lead them to have an interest in prompting all commercial entities
to maintain a Software Bill of Materials (SBOM) in their IT system so that they can add identify elements
in their systems, address vulnerabilities, and ensure updated systems. Requiring SBOMs would also
present a way for insurers to understand their aggregated portfolio exposure to a given technology and
defend their insured tech companies from performance violations that tech customers allege. This
symbiotic relationship of risk identification and management among the insured customers on both
sides of the tech relationship, that is the tech providers and users, may be hard to institute today given
all the information required to be stored and assessed and the many nuances of threats, vulnerabilities,
responses and behaviors that need to be factored into an assessment. In the future, big data and AI could
well help support this approach and drive more public-private as well as private-private partnerships in
data and experience sharing. The good news is that the insurance industry is already being innovative in
using AI and in developing AI insurance solutions for AI developers and users.
INSURERS’ NEED TO HELP ADDRESS RANSOMWARE

The insurance industry has been criticized for paying when ransomware strikes their clients. However, Marsh notes the payment of ransomware is a customer decision and attackers do not necessarily seek out those who are insured. The insurance broker also notes that, although ransom attacks have increased, payouts as a percentage of attacks have declined largely due to the enhanced controls, such as strong backup protocols, that insureds are now being required to have to qualify for coverage. Nonetheless, hackers can infiltrate, and have infiltrated according to one industry source, companies’ systems to find details of the target’s insurance policies. Royal United Services Institute (RUSI), a London-based think tank, did a yearlong study of ransomware payouts and their relationship to cyber insurance. Published in 2023, RUSI’s study found “no compelling evidence that victims with cyber insurance are much more likely to pay ransoms than those without.” However, the study noted the need to have better ransomware reporting to authorities, which insurers could require of policyholders, and recommended, among other things, that insurers work to develop and identify best practices in ransomware responses and seek the possible development and use of specialist ransomware response firms.

The U.S. Counter Ransomware Initiative at its November 2023 meeting rightly committed the participating states to closer engagement with the insurance industry on addressing ransomware and to the encouragement of ransomware reporting. In an innovative move, France amended its laws to allow ransomware payouts under insurance only to entities that have informed authorities of an incident within 72 hours. As the U.S. moves toward some required reporting of ransomware, it is relaunching its Cybersecurity Insurance and Data Analysis Working Group (CIDAWG) to help identify ways to “drive down cyber risks” and to work at this effort collectively. In the United States, proposed rules for critical infrastructure reporting of incidents, including ransomware, are open for comment through July 2024. However, the issue of an outright ban for all on ransomware payments is not considered realistic.

The issue from the insurance industry side is what companies or associations are best placed and willing to engage and to help drive needed changes across the industry.

INSURERS’ CONCERNS CAN DRIVE WORK TO IDENTIFY AND MANAGE SYSTEMIC RISKS AND KEEP THE INDUSTRY VIABLE

Insurance is one of the biggest industries in the world. The Financial Stability Board (FSB), formalized during the 2008 financial crisis, promoted more standardization of financial regulation to include oversight of insurers to avoid future global financial shocks. Thus, maintaining a healthy insurance industry globally is important. The question is how to achieve this goal given the nascent understanding of current/emerging digital risks.

While insurers have long worried about being overexposed to an industry, region, or market change such as interest rates, those systematic risks differ from growing concerns over systemic risks. Systemic risks can have cascading and often unexpected or difficult effects to predict and assess due to connections among entities and systems—and can be complex or otherwise obfuscated from insurers’ view. These risks can be less known but are widely used, like the Log4j piece of open-source software that was found to have vulnerabilities. Systemic risks can also stem from catastrophic events, like an attack on the underlying structure of the internet or something more directed like the takedown of a financial payments
system. Now AI has become a concern for compounding malicious actors’ targeting abilities. Some work is underway to help identify systemic risks, including funding from re/insurers (noted earlier), the World Economic Forum being an important hub of research, and the Carnegie Endowment for International Peace also working on systemic risks, insurance, and attribution.

Better risk modeling alone cannot address managing risk accumulation from cyber-related systemic events. This fact has limited the growth in affordable cyber coverage. The Geneva Association, an international association of insurance companies, noted in its comprehensive paper on cyber risks, “Insurers are employing stricter contract wording and maintaining low policy limits [in comparison to limits provided on other types of commercial insurance], but with potential cyber exposures only set to grow, this implies a huge and persistent protection gap.”

Part of this gap had been due to reinsurers, to whom insurers lay off some risks, not being willing to take up some of those cyber exposures. That reality has been changing as insurers insist clients have better risk management and require tighter contract wording. However, the tail risks—those low-probability but high-consequence events—persist and constrain primary as well as reinsurance policies.

One of those tail risks involves wars. The historic general insurance exclusion for “hostile” or “warlike acts” persisted in insurance policies until the 2017 NotPetya virus, which originally targeted Ukraine, spread to others and caused significant losses; that led to global claims under all-risk policies, as the attacks were attributed to Russia. Yearslong litigation ended in out-of-court settlements for two large claims by Merck (a pharmaceutical company) and Mondelez (one of the world’s largest snack food companies) and their insurers. Lloyds of London (a specialist insurance and reinsurance market) now requires all policies underwritten by its syndicates not to be silent on the potential cyber exposures covered and to state clearly whether policies affirm coverage for cyber incidents. Lloyd’s has required that all policies, including cyber policies, clearly and directly address how policies are to address events linked to sovereign states involved in wars, whether declared or not, or state-backed threat group activity. However, some have asked for more clarity on these definitions.

The U.S. government has been considering a risk-sharing scheme in which the federal government “backstops”—that is, provides funding support—against catastrophic losses, akin to the Terrorism Risk Insurance shared-risk model or the National Flood Insurance Program. The goal would be to broaden the availability and affordability of cyber reinsurance but without promoting moral hazard. Indications are that the insurance market’s development, including through new mechanisms like insurance-linked securities (ILS), may well provide added market capacity to allow the industry to absorb more risks. However, a wait-and-see approach chances a major cyber event occurring before the market—and its support for restoring business functions—has evolved sufficiently. Any government support program has an element of moral hazard in it, as does all insurance including ILSs. However, the triggers and terms of both these mechanisms can help to manage the risks. For example, any backstop should consider being available only to re/insurers who require certain levels of security from those insured, thus helping to drive greater overall cybersecurity. In addition, rating agencies will become increasingly a focus as they give ratings that help drive the pricing of ILS; the question then becomes how well they are able to rate them.
Key Takeaways and Recommendations

1. **Strengthen insurance as a mechanism to promote accountability.**

   Insurance is an important tool for promoting accountability in cyberspace but can be strengthened. Several efforts should be considered to support this objective. The plan within the Counter Ransomware Initiative to engage with insurers needs to be jump-started and expanded to both a public-private and private-private partnership. For example, a series of roundtable discussions of representative insurers, brokers, customers, and others could be held to address some of the outstanding insurance ideas and concerns.

2. **Require and standardize incident reporting and processes for better risk analysis and management.**

   Incident reporting is needed in a responsible manner and should be standardized to allow for better risk assessments and management by all stakeholders, including law enforcement. Efforts to require reporting are moving forward in a piecemeal fashion with many informal efforts to gather incident data, including in academia and from NGOs. Some states and organizations are requiring ransomware and other incident reporting that is not necessarily consistent even within a state.\(^5\)

   The U.S. and other countries are requiring reporting of ransomware and other cyber incidents from certain entities such as critical infrastructure. There is sometimes a stigma when investors see systems as being vulnerable to cyber threats which leads to lower ratings or stock prices, or customer insecurity. Required reporting could help erase the stigma of vulnerable systems and lead to more effective monitoring of the threat landscape thereby benefiting all entities and law enforcement.\(^5\) It would also help insurers/academics/tech firms in their risk research to build better models for security protections. In the short term, the French approach of requiring confidential reporting to authorities of ransomware attacks as a prerequisite of insurance payout might be expanded internationally. A pilot program to expand and systematize such reporting could be developed working with appropriate stakeholders, possibly through the International Counter Ransomware Task Force, part of the Counter Ransomware Initiative, and leveraging the Financial Action Task Force (FATF) in its work on cryptocurrency, which is the primary source of ransom payments.\(^5\)

   As specialist companies have developed to negotiate and facilitate ransom payments, some industry standards could be developed to require these companies to follow agreed practices in accordance with guidelines from FATF and others to ensure sanctions’ enforcement.

   In the longer term, incident reporting might be expanded beyond ransomware. The Organization for Economic Cooperation and Development (OECD) has been very forward-thinking in developing an approach to define and monitor AI risks;\(^5\) it is not too late to have centralized coordination around cyber risks.

3. **Require more consistent minimum conditions and definitions for coverage/benefits.**

   Re/insurers evaluate those to whom coverage is provided. How this process is managed is critical to both industry health and capacity as well as incentive structures for insurance clients and for insurers. Within the industry, some guidelines/standards have been set for coverage clauses to better manage
risks and operating losses and to better attract reinsurers for risk sharing and increased capacity. Whereas underwriters want to know a lot, applicants want to minimize the application process causing a competitive dynamic between customers and insurers that needs careful management. In other risk areas, some insurance service providers have forms the industry traditionally uses to provide quotes.\textsuperscript{60} Simply standardizing some of the questions and policy wording would be a welcome evolution of the cyber insurance market and would help buyers understand the risks they have and their coverage.\textsuperscript{61} This standardization could be done by leveraging new technological approaches and AI.\textsuperscript{62} Whether this approach could be agreed in the industry is an open question.

A critical issue is the imprecision in defining exclusions and limits, such as for war/warlike acts, attribution and its methods, what constitutes an impacted state, and what should be considered as a major impact. Lloyds has provided some guidance, but more questions persist on policy terms.\textsuperscript{63}

The issue of catastrophic losses from systemic risks looms large. A coordinated effort to explore and define the above terms within the context of systemic risks and how to manage them is needed, including identifying the elements of best practices for the insured. Those practices should change dynamically as technology and knowledge evolves. Increasing the liability of tech providers for their services/products will be an element of this effort. States should consider affording liability limits—or safe havens—to those following agreed good practices. Further, if some states decide to provide support to the insurance industry through a backstop that would cover some industry losses, then the states and stakeholders must clearly define the technical characteristics of systemic risks. This reality may obviate some complicated current policy requirements for political attribution and support the development of a coordinated effort toward some accountability.

Having an independent body determine attribution is something that the UN and historically the OECD have suggested. However, before that happens, the insurance industry needs guidance. Technical characterizations of systemic risks without the constraints of legal and political attribution could serve the industry well and help jump-start other international processes toward a robust, transparent, and accepted framework for accountability for supporting cyber norms.\textsuperscript{64}

4. Expand understanding and availability of catastrophic cyber risk mechanisms with clear terms in backstops and triggers.

The insurance industry adapts to new risks, with some always willing to provide insurance where others may not and with new catastrophic risk instruments developing such as insurance-linked securities. As noted above, systemic risks are an inhibiting issue for insurers and reinsurers alike. As reinsurers attempt to manage their portfolio risk for cyber policies, and insured organizations continue to gain a better understanding of the exposure and potential for loss, there will continue to be a need for greater availability of capacity in the cyber insurance marketplace. To allow for expansion of capacity in the cyber insurance market, it will be necessary to expand the availability of mechanisms that allow insurers to better manage the potential of catastrophic cyber events. Currently, insurers have relatively limited options when it comes to managing catastrophic cyber risk, with most choosing to purchase reinsurance. In 2023, the market began to see some insurers pursue catastrophe bonds as an alternative to purely transferring risk to a reinsurer.\textsuperscript{65} Growing interest in ILS would allow insurers another opportunity to manage catastrophic risk through the issuance of securities whose performance is tied to the results of the underlying insurance portfolio.
The possible role of rating agencies in assessing re/insurers processes for managing risks and issuing policies needs to be further explored.\textsuperscript{66} With the advent of big data, rating agencies are expected to increasingly help drive better cybersecurity practices across industries,\textsuperscript{67} including within the insurance industry, as they rate ILS for the benefit of capital market investors.\textsuperscript{68}

Market incentives such as insurance have a great untapped potential to strengthen cybersecurity norms and laws. These incentives just need to be further explored and harnessed.

Endnotes

1 Note that there are different types of insurance companies, including publicly traded insurers, mutual insurers that are owned by their policyholders, and others. These companies are regulated in different ways internationally. Underwriters help assess the risks these companies take on.

2 “Commercial Insurance : Information,” Insurance Information Institute, \url{https://www.iii.org/publications/commercial-insurance/introduction}.

3 Note that insurance does not cover the criminal acts of the policyholders themselves.

4 These “affirmative cyber insurance policies” can be stand-alone policies or included as specific endorsements to existing property and casualty (P&C) policies and evolved from initially focusing on third-party liability (harms to others) to first-party losses (harms suffered by the insured and cover losses to self).


8 Twelve key controls were developed—with one added for manufacturers and their operational technology, Marsh, “Cyber resilience: Twelve key controls to strengthen your security,” April 2022, \url{https://www.marsh.com/es/en/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html}.


For an explanation of professional indemnity and errors and omissions (E&O) coverage, see: “Clearing up the differences between E&O and PI,” ANZiF, September 20, 2022, https://anzif.com/professional-development/articles/2022/09/clearing-up-the-differences-between-eo-and-pi.


The US SAFETY Act provides limitations on the liability of entities for products, systems, and services, such as providing security at a football game, for those that receive certification. See: “Safety Act,” Homeland Security, https://safetyact.gov/.


57 In 2023, the FBI reported that the internationally coordinated takedown of Hive, the ransomware-as-a-service platform, returned over $100 million to victims of ransomware and that, during the FBI’s monitoring of Hive, only 20% of entities had reported the ransoms to authorities. See: Toney Riley, “FBI seizes Hive ransomware group infrastructure after lurking in servers for months,” Cyberscoop, January 26, 2023, https://cyberscoop.com/fbi-europol-hive-ransomware-group/.
For information on the International Counter Ransomware Task Force, see https://counter-ransomware.org/aboutus.

“Overview,” OECD AI Incidents Monitor: OECD AI, https://oecd.ai/en/incidents-methodology. This includes, for example, “severity, industry, related AI Principle, types of harms and affected stakeholders.”


Some have suggested using technographic data.


This includes so-called 144 bonds that allow for trading. See: “Rule 144A Catastrophe Bond,” Artemis, https://www.artemis_bm/glossary/rule-144a-catastrophe-bond/.


11. The International Telecommunications Union

Allison Pytlak and Shreya Lad*

The International Telecommunications Union (ITU) is the United Nations (UN) specialized agency for information and communications technologies (ICTs). It is an intergovernmental organization with a technical focus and regulatory function. While it has not played as central of a role in UN dialogues about state use of ICTs in the context of international peace and security as some other bodies have, it is nonetheless an important actor with long-established legitimacy as a trusted and competent governance body and platform for general ICT standardization and regulation.

What is the ITU?

Founded in 1865 by a group of 20 European states at the dawn of the telegraph era, the organization that came to be called the International Telecommunications Union (ITU) officially became a part of the United Nations (UN) in 1942, making it the oldest agency of the organization. Over time, the ITU has gained importance for its work in standardizing technologies such as telegrams, telephones, radios, and satellites as well as building out communications capabilities of its member states. In the 21st century, the ITU remains a crucial global platform, shaping telecommunications on various levels.

The ITU consists of two types of members: member states, encompassing 193 countries, and sector members, comprising roughly 900 private-sector corporations. This latter category is per a 1994 ITU constitutional change, which allowed nongovernmental actors from the private sector to join the ITU. Sector members are active in the subsidiary bodies of the ITU, but do not have voting rights in the ITU plenipotentiary conferences. ITU sector members come mainly from the private sector, the technical community, and academia.

Oversight is provided by the ITU Secretary-General who collaborates closely with the ITU Council, an elected entity composed of a quarter of the member states. Every four years, member states assemble for a plenipotentiary conference, a platform for decisions on elections, strategic plans, and financial affairs. At plenipotentiary conferences, recommendations are turned into resolutions, which are voted on by council members. These resolutions hold significant consequences for global ICT regulation, standards, and policies.

*This case study is based on initial research prepared by Christopher Barclay, a 2023 Stimson Center intern. Barclay’s research examined political dynamics within the ITU and the impact on its role in UN cyber governance efforts.
The ITU’s operations revolve around three technical sectors: a Telecommunication Standardization Sector (ITU-T), dedicated to international standards concerning topics such as internet connectivity and 5G technology; a Radiocommunication Sector (ITU-R), responsible for managing radio systems, including satellite ownership and spectrum allocation; and the Development Sector (ITU-D), offering technical and capacity services to close the digital divide and drive digital transformation.5

Relevance to Cyber

In response to evolving concerns about cyber threats and misuse of ICTs, the World Summit on the Information Society (WSIS) was established by the UN and was initiated by the ITU through a two-phase summit in 2003 to establish a shared framework for viewing and regulating ICTs across countries.6 The WSIS allocated specific roles to various UN agencies for ICT regulation. In this context, its Action Line C5 tasked the ITU with the role in “building confidence and security in the use of ICTs.” As a result, the ITU launched an effort called the Global Cybersecurity Agenda (GCA) to fulfill this mission. The GCA is built upon five pillars: legal measures; technical & procedural measures; organizational structures; capacity-building; and international cooperation.8

Action Line C5 also emphasized the ITU’s responsibility for fostering topics such as global collaboration on trust, data protection, preventing the misuse of ICTs, and encouraging UN engagement in enhancing ICT security.

The ITU has developed an extensive program on cybersecurity. Three activities are particularly relevant for promoting accountability in cyberspace: the Global Cybersecurity Index, National Cybersecurity Strategies, and the National CIRT program. These efforts are described below.

GLOBAL CYBERSECURITY INDEX

The Global Cybersecurity Index (GCI) was initiated in 2015 under the framework set out by the earlier 2007 Global Cybersecurity Agenda. The description on the ITU’s webpage states that the GCI is a “trusted reference that measures the commitment of countries to cybersecurity at a global level—to raise awareness of the importance and different dimensions of the issue.”9 This Index is used to identify areas of strength and growth in cybersecurity and to highlight good practices, as well as cybersecurity commitments for member states to implement as suitable to their national environment. As stated in ITU Plenipotentiary Resolution 130, the ultimate goal of the Index is to foster a global culture of cybersecurity and the integration of cybersecurity at the core of information and communication technologies.10

The index has four editions so far, with a fifth edition scheduled to be released later in 2024.11 It reflects a consultative process that starts with the development of a questionnaire, which is revised and adapted on the basis of inputs received from member states and the GCI Expert Group (earlier editions included a GCI Correspondence Group, now part of the Expert Group). Member states are invited to participate by designating focal points for data collection. Responses are collected through an online portal. The Telecommunication Development Bureau (BDT) Secretariat conducts secondary data collection, refines responses, and produces a validated questionnaire for analysis. For countries that did not respond to the questionnaire, publicly available data and online research form the basis of collected data, which are
reviewed and validated where possible. The process culminates in a report that summarizes trends and best practices of ITU member states around the world.

The Index’s conceptual framework is based around the same five pillars of the GCA: legal measures, technical and procedural measures, organizational structures, capacity-building, and international cooperation.

The GCI was recently restructured into levels of commitment, moving away from rankings to provide a more meaningful assessment of countries’ strengths and areas for improvement. Between 2015 and 2024, the number of member states participating in the GCI grew from 105 to 172 countries.

The Index has been a valuable contribution to identifying areas for improvement and promoting the adoption of best practices in cybersecurity. Further, the Index complements other, ongoing efforts taken by countries, companies, civil society organizations, and individuals to ensure a secure cyberspace.

**NATIONAL CYBERSECURITY STRATEGY DEVELOPMENT**

Robust national cybersecurity strategies can play a vital role in fostering secure and resilient digital growth, especially in developing nations. Building on the established GCI framework, the ITU supports countries in crafting effective national strategies.

To provide countries with a clear framework for developing their national strategies, the ITU led a group of 25 organizations in developing a Guide to Developing an NCS, currently in its second edition. The NCS guide forms the basis for ITU’s BDT and the work of other implementing organizations when supporting countries’ efforts to develop or update their national cybersecurity strategies. The guide is scheduled for revision in 2025 to reflect evolving technology and policy needs and has been accompanied by a series of online trainings.

The guide’s strength lies in its demonstrated ability to provide a standardized approach for various implementing agencies, ensuring consistency across implementation efforts. Furthermore, the guide is designed to be adaptable to each country’s specific political, economic, and social context and can be independently used by countries. This adaptability guarantees that strategies developed have local ownership and meet local needs.

**NATIONAL CIRT PROGRAM AND ACTIVITIES**

National Computer Incident Response Teams (CIRTs) serve as a national focal point for coordinating cybersecurity incident response within a country. The ITU works with its member states to build capacity at national and regional levels. One way in which it does so is through a CIRT assessment, which helps to define a state’s readiness to implement a national CIRT. After the CIRT assessment, the ITU assists with planning, implementation, and operation of the CIRT. At the time of writing, the ITU has completed assessments for 80 countries and helped to establish or enhance CIRTs in 17 countries. The ITU’s CIRT framework helps to break down the phases of CIRT development through to establishment and provide ongoing support and maintenance. Within the framework, the role of different stakeholders with respect to national CIRTs are identified and clarified.
National CIRTs are an excellent way to assess threats in environments with capacity constraints and to develop a path forward toward resilience and positive accountability. As an emergency response mechanism, the CIRT initiative models accountability, both in terms of outlining the best practices that states can undertake based on their baseline capabilities, as well as preventative/responsive measures to crises. They also incentivize reporting in a timely manner.

**Key Takeaways and Recommendations**

Existing ITU activities and projects such as those described here could be better leveraged and recognized for their contribution toward building accountability, particularly positive accountability. For example, and as noted online, the GCI provides a “complement to other measures related to cybersecurity by enabling countries to identify where action has been taken, what action may be insufficient, and how to understand the landscape of successes.” Such benchmarking and monitoring of capabilities, priorities, and needs is a core aspect of accountability.

Bolstering the capacity of national CIRTs and national cybersecurity strategies—core components of responsible behavior—correlates to positive accountability. National CIRTs model accountability, both in terms of outlining the best practices states can undertake based on their baseline capabilities, as well as preventative/responsive measures to crises. Effective national mechanisms and institutional structures are vital for reliable and effective responses to cyber threats and incidents.

While not studied in detail as a part of this case study, the ITU’s growing body of work to promote gender diversity in the field of cybersecurity can also be seen to bolster accountability. An aspect of accountability is considering the crucial question: who is accountable to whom, which must include historically marginalized individuals or communities that are too often left out of cybersecurity policymaking or technical activities yet can be disproportionately impacted by malicious cyber activity. Moreover, due to the inherently multistakeholder nature of cyberspace, the involvement of multiple stakeholders, including private entities and civil society, is imperative for comprehensive regulation. The approach of the ITU in allowing nongovernmental actors to participate is noteworthy, although the preference given to the private sector reduces the impact and participation of other types of stakeholders. As with any international organization, the ITU is not immune to the geopolitical challenges that often beset such organizations, not least in the area of international cybersecurity. Yet, its long-standing role as a governance body and platform for ICT standardization and regulation more generally represent core components of efforts to globally advance cyber accountability.
Endnotes

1 For more on the history of the ITU, see G. Balbi & A. Fickers, eds., 2020, “History of the International Telecommunication Union (ITU),” Transnational techno-diplomacy from the telegraph to the Internet, (Berlin: De Gruyter).


11 ITU, “Global Cybersecurity Index.”


14 Ibid.


Conclusions

Allison Pytlak and James Siebens

This report has examined several mechanisms from diverse issue areas to identify good practice in the area of accountability that could be instructive or relevant for cyber. Every case study has offered its own conclusions and recommendations. In combination, these cases represent a rich menu of policy approaches that have already proven valuable to varying degrees in structuring incentives to better manage difficult transnational security and governance challenges of common concern, and indeed, common consequence and responsibility for the international community.

Drawing on the case study-specific conclusions and recommendations, this final section of the report offers six cross-cutting and overarching conclusions for cyber accountability and four other pertinent observations. We also list several possible models (frameworks and mechanisms) that we believe have value for addressing particular accountability cyber gaps and challenges. Finally, we identify other areas for future research.

Overarching Findings

1. There is no ‘one size fits all’ solution for cyber accountability gaps. An integrated ‘regime approach’ comprised of mutually reinforcing mechanisms, tools, and levers is a promising approach for cyber governance given the diverse needs, threats, and gaps that exist.

Based on multiple case studies, it is evident that mixed and ‘integrated regime’ approaches offer unique value for enhancing accountability and reducing harm. It does so by designing and incorporating mechanisms that can be focused on particular concerns or threats, and that account for a landscape with diverse threat actors, as well as diverse stakeholders and participants. For example, such an approach has been useful in arms control and nonproliferation efforts which are similarly composed of formal and informal mechanisms, including legally binding agreements as well as informal trust-building measures and information-sharing, among other activities and agreements. Outer space governance presents a similar approach.

In cyber, such a mixed approach leverages both positive and negative incentives and can also involve different accountability layers and types. It will allow for formal and informal mechanisms, including those that depend on market incentives to encourage positive behaviors among private actors.
To a large extent, a loose regime approach is what already exists in cyber governance. While international law and the UN norms provide a universal baseline for states, there are a multitude of other mechanisms which variously focus on particular threats and concerns or are open to particular types of constituents. This is also reflected in the approaches of certain regional actors, such as the European Union and its Cyber Diplomacy Toolbox, or the African Union’s shared interpretation about the applicability of international law to state use of ICTs. The emerging integrated regime approach reflects that States and stakeholders have differing priorities and capacities in relation to accountability initiatives.

When applied to accountability, this approach helps the international community to broaden understanding of the term beyond simply attributing malicious acts and punishing perpetrators. Accountability is needed to reinforce the positive actions that can be taken to support cyber security and responsible behavior as well as for ensuring negative acts are deterred, disrupted, and disincentivized. States, service providers, and users of cyberspace need to be accountable to relevant commitments and to different stakeholders.

Yet there is a very real risk of having too many tools in the box, however, and either not employing any of them thoroughly enough or creating loopholes and contradictions between their provisions that might be exploited. Too many tools may also send mixed messages about expectations of what is and what is not
acceptable behavior, further exacerbating accountability gaps and risking unanticipated or unintentional escalation. Some of the case studies demonstrated where so-called harmonizing instruments have added value by clarifying and streamlining expectations and closing loopholes.

2. Focusing on activities and behavior offers more potential than focusing on the means and technologies.

Several case studies illustrated the benefits of policy and regulation that focuses on activities and behavior, rather than on items and technologies. This could be impactful for improving cyber accountability because it helps to mitigate the loopholes and challenges posed by constant technological change, in which efforts to prevent or address harms posed by a particular technology will always lag behind policymaking. Such a focus aids in addressing the dilemma posed by dual-use items, since the latter can seamlessly alternate between 'military' and 'civilian' applications, and 'wartime' and 'peacetime' uses. In this regard, an updated understanding of “dual-use” for the digital era is warranted.

This approach may also be instructive for determining what is unacceptable as based on impact or harm, such as through a human rights or peace and security lens and it offers applications for positive and negative accountability.

Yet, despite this finding, it bears mention that views about tech neutrality are not universal. A significant amount of research has illustrated the racial, gender, and other biases implicit in some technologies or the datasets which underpin, or in unequal access to technologies. Calls from UN experts for moratoria on items like surveillance software spyware has also made the point that some software has only malicious and harmful uses and should not be seen as neutral. While a tech neutral approach may be best way forward, broadly, there are instances where the technology in question is problematic.

3. Cross-domain governance could be better leveraged to advance accountability.

From human rights to outer space and the use of private security companies, there are cyber and digital related risks inherent in many of the case studies explored. To this end, we propose that cross-domain governance could be better leveraged to advance accountability. For example, a better integration of digital and cyber threats within human rights peer review processes such as the Universal Periodic Review (UPR) could aid in the meaningful operationalization of UN cyber norms on human rights and the broader applicability of international human rights law (IHRL) to cyber.

Cyber security may have positive and negative knock-on effects for other domains and could spearhead discussions on accountability in militarized or sensitive domains. For instance, how does an antisatellite test ban implicate the use of cyber tools for counterspace targeting? Given the cross-domain connections between cyberspace and outer space, it is reasonable to examine what strong mutual priorities are functioning well in space and see if they might be similarly suited for building consensus around observing global cyber norms.

Stimson’s research has further affirmed that States weight their priorities as a whole, meaning that considerations in cyberspace are often a result of risks faced in other domains or in relation to other
objectives and priorities. As such, incentivizing responsible behavior across domains could help fill in cyber accountability gaps.

One potential risk that emerged through our research is that greater cross-domain governance will multiply the number of actors involved, which could make it challenging to bring about a focused result on cyber accountability and the actors particularly involved in cyber activities of concern.

Another take on ‘cross domain’ is not about issue areas or global commons, but rather about the relationship between the military and private sector domains. As militaries increasingly rely on private sector services and equipment because they are faster, cheaper and easier to acquire, commercial and military assets are increasingly comingle, which blurs accountability and responsibility.

4. Inclusivity is imperative when developing and implementing cyber accountability mechanisms and for ensuring effective governance more broadly.

Across the board, cases studied demonstrated successful engagement with a breadth of nongovernmental stakeholders, through a diversity of methods and on issues as equally sensitive as cyber peace and security. In most of these cases the engagement was not merely successful in a superficial or tokenistic way, but rather it added real value and, in many instances, aided in fostering accountability. In some mechanisms or issue areas this was in relation to early phases of developing new policy or law, such as through advocacy or lending technical expertise; or in other cases nongovernmental stakeholders brought value by supporting practically, or monitoring implementation of agreed commitments. Within this, an important lesson learned is that inclusivity is most effective when there is clarity around roles and responsibilities of different stakeholders.

Given the inherently multistakeholder nature of cyberspace, this is an important and relevant finding. Many of the forums where cyber laws and policies are enacted are largely inclusive, but this is not universal and, in some cases, the participation of nongovernmental stakeholders has been challenging.

What does this mean for accountability? One of the first requirements is to identify and understand the differing roles that diverse stakeholders play in fostering accountability. This includes in relation to building awareness of and supporting implementation of agreed norms and law. Some actors can be held accountable through peer reviews and other mechanisms, which may be initiated or involve nongovernmental stakeholders. Tech providers can develop transparent industry performance principles and best practices such as security by design as an integral part of development rather than an add-on. Insurers can develop more standardized processes to hold their clients accountable, for example, through compliance with certain standards and vulnerability risk assessments. More broadly, the enterprises that comprise the layers of the internet — from IP addresses to routing — should also be part of accountability. Other stakeholders have a role to play in reporting about cyber harm and raising awareness about responsible behavior and legal obligations.

Best practices for inclusivity should be upheld within cyber policy-making forums. Inclusivity should be reflective of different types of stakeholders as well as consider gender, racial, linguistic, and other forms of diversity. The work of Global Partners Digital and Association for Progressive Communications about inclusivity and cyber norm development, are some examples of working being undertaken in this area.
Inclusion of experts and practitioners in the development of new frameworks, new norms, or updating existing mechanisms to ensure their real-world efficacy and enhance credibility.

A particular role those nongovernmental actors played in some of the mechanisms studied (Montreal Protocol, ICoCA, APRM, and insurance) was in providing independent validation and assessment. These case studies indicated that expert support for a range of activities, from risk assessment to validation and verification, helped to avoid concerns over politicization in developing technical characterizations and guidance to policymakers, and in ensuring compliance. Independent risk analyses and assessments can create specialized channels for monitoring, verification, and implementation.

In cyber, such independent bodies could be useful for depoliticizing attribution processes. That said, there is a risk that independent bodies may not be provided with the correct information, or all the information needed to perform an attribution, given that often this comes from classified information and intelligence. Should such bodies arrive at incorrect or false conclusions, accountability and trust would be negatively impacted.

5. Carrots and sticks.

Several case studies illustrate the need for a range of ‘carrots and sticks’ to drive incentive to comply with commitments and obligations. These range from market incentives to other forms of rewards, such as the potential of capacity-building or other support as well as reputational considerations, but also penalties and costs.

Successful accountability in cyber governance likewise requires consideration of incentives and repercussions, not far removed from the concepts of positive and negative accountability. Such carrots and sticks should be designed with a view towards the specific community of actors involved or targeted.

It will be necessary to find ways to elevate cyber security investment as a key priority for states and stakeholders. A way to do this are the development of cost-benefit models to identify the costs, in terms of financial and other harms, to companies, states and societies of incidents and the reduction of these from selected actions and/or activities. These could be done by expert groups.

Positive incentives are needed to adopt and operationalize norms, and to interpret and apply international law. States can be supported to prioritize security investments through some explicit means, such as technology transfers, infrastructure development assistance, or sanctions relief. The true cost of malicious cyber incidents, including losses—in time, money and reputation—is not well appreciated or documented. Sustained investment in the cyber security of states and other organizations can pay dividends, including for economic development.

With adjustments in coverage, insurance could also play a role, as underwriters develop clearer understandings of risks and collaborate among themselves. Insurers also have an interest in defining systemic risks and warlike acts in order to better manage their exposure. To give the insured benefits of good security investments, the industry could explore standardized safety certificates, coordinated stress tests, vendor reviews, liability reforms, as well as the adoption of international frameworks and collaborative partnerships among businesses and states.
Incentives for the private sector and civil society to be resilient are needed as well, which will necessarily be more tailored to their specific needs and interests.

6. Political will is a must.

Ultimately, the key variable with all such efforts is political will to not only constrain the behavior of others through regulations and a compelling combination of carrots and sticks, but also for capable actors—governments and private actors alike—to exercise mutual restraint in their uses of such technologies.

We have observed that states have a higher appetite to discuss issues and uphold commitments that do not directly implicate themselves. In cyber, this has tended to include topics like cybercrime, commercially available intrusion capabilities, and not attacking critical infrastructure. While these threats and threat actors do not represent the full spectrum of cyber challenges, they might constitute a starting point for cooperation among states and other stakeholders, and where there is a greater willingness to hold one another to account because political will exists at a higher level.

With respect to activities like attribution, there may be greater political appetite for calling out/condemning impacts and effects, or behaviors, rather than naming and shaming an actor.

Other, non-cyber elements in bilateral and multilateral State relationships can affect their cooperation in the cyber domain. Domestically, states also have differences in values and how they drive decisions. This intersects with political will and appetite for cyber issues.

There does not appear to be a perfect formula for generating political will—and indeed, in any of the issues areas researched this is a problem—but the research does point to good practice such as ensuring buy-in and ownership when developing policies, regulation or law; considering the barriers for entering into frameworks or mechanisms; and understanding that states and stakeholders will have differing priorities and capacities in relation to accountability initiatives.

Other Pertinent Observations

Capacity building

The research process affirmed multiple times that capacity building is foundational for all aspects of cyber security and resilience, and therefore has a role in accountability, especially positive accountability and as “deterrence by denial”. It should be planned and carried out in accordance with states’ desired outcomes rather than their current capabilities. A gap analysis of national needs and priorities, as well as a common vision of achievable objectives for different stakeholders, would assist states in identifying the most important and viable areas to undertake capacity building in the near term.

Yet capacity building is not always as apolitical as one would like or imagine it to be. Some states fear that another state is loaning its support for capacity to advance their general power, and it becomes a geopolitical issue. The research process also revealed challenges in performing needs assessments and
gap analysis of national needs and priorities, as well as a common vision of achievable objectives for different stakeholders, would assist states in identifying the most important and viable areas to undertake capacity building in the near term.

Capacity building by and for all types of stakeholders is needed. To hold actors to account, it is essential to possess the requisite resources, skills, and authority. For states seeking to embody responsible behavior, more detailed principles and guidance are needed. Capacity building should seek to bridge the gap between authority (actors with the agency and access but not the capabilities to achieve objectives) and resources (actors with the capabilities and expertise but not the authority or resources).

Adaptability

Adaptability is a fundamental principle of a successful and dynamic governing mechanism which can aid in accountability. Based on our research, mechanisms require clear definitions and an overarching structure to ensure accountability. However, mechanisms also need to consider review processes or other ways to be adaptable in step with new information or technologies that evolve whether that is scientific (as in the case of ozone) or experiential (as in the case of UNSCR 1540, the Wassenaar Arrangement, and GDPR). Adaptability includes recognizing the limitations of working through a UN or political system that requires consensus.

In some ways this also mitigates the challenge of how policy can keep up with technological development, although it bears mention that even with adaptable mechanisms, new technologies can still be misused. Therefore, a focus on behaviors (see Finding #2) and accounting for adaptability can increase the prospects of accountability.

Likeminded coalitions and regional initiatives

A theme that surfaced repeatedly throughout the research process, and with conflicting findings, is around the value of regional approaches and working in smaller, like-minded coalitions. Often these approaches are shown to be relatively more straightforward to establish because they are based on common values, interests, and concerns, or pre-existing channels of communication that aid with trust and confidence.

This was found to be true in some of the case studies (APRM, GDPR) but also exists in cyber through regional initiatives or collaboration, and through coalitions such as the Counter Ransomware Initiative, the Pall Mall Process, the Cyber Security Tech Accords, or even joint attribution statements. In these instances, questions remain about the impact on accountability beyond their membership—while the similarities amongst members make it easier to develop frameworks or set policies initially, can they be universalized? How to ensure cohesion with other frameworks from other groupings? Are initiatives from small like-minded coalitions able to influence or bring along parties that are not like-minded or middle ground? It has also been noted that often it is the specificity of activities that coalitions and groupings seek to deter or disrupt is what makes them attractive, particularly when it’s an issue of wide concern to many (i.e. ransomware).
Stimson Center-convened discussions about accountability in 2023-24 raised further points on this topic. It was noted that for smaller countries or nongovernmental stakeholder groups, it can be challenging to decide and prioritize which coalitions or networks to join, and that often a “big tent” approach (i.e. forums that are less specific in topic and bring in more actors) are preferrable. Others noted it is precisely because of limited resources and capacity that coalition action is so important.

Definitions and clarifications

Throughout our research process, the topic of definitions surfaced often. Agreed definitions on certain terms and types of operations could bring clarity in some contexts, while others noted this might only further encourage malicious actors to pursue operations in a grey zone. The political and other challenges of reaching agreed definitions were also noted. Some believed that having clear definitions while ensuring strong, yet unspecified responses could deter malicious behavior. At present, strategic ambiguity appears to be the favored approach. These concerns raised questions regarding whether and how to shift toward an incentive framework that rewards clarity and commitment. More detailed principles and guidance are needed for states to understand how to demonstrate positive behavior, not just acceptable behavior.

The need for more consistently defined and/or widely understood definitions of cyber harm or impact was also pointed out as aiding in accountability, because such understanding could help to reinforce thresholds for unacceptable behavior. When defining harm, it is important to recognize the various types and levels of harm. It is also necessary to identify incidents that have a significant impact as well as those that have relatively lower-level effects but affect a larger number of individuals, cumulatively. Identification of specific groups that suffer harm should also be noted rather than neglected, including at-risk populations. To this end, efforts such as those being led by the CyberPeace Institute to develop a common harms methodology are welcome.

Many in civil society want more clarity from states and technology companies, particularly regarding operating standards, principles, and what constitutes responsible behavior. They aspire to have more input into policy-making discussions. The initiative being led by the Royal United Services Institute (RUSI) to map practical understanding of responsible behavior can aid in this, as one example.

Possible Models

As noted earlier, this report does not seek to recommend one mechanism or instrument to ‘solve’ cyber accountability, or as offering greater value than others. In fact, in keeping with the finding about an integrated regime approach, we believe that different responses and tools are needed for different gaps and challenges. In that spirit, our research process over the last fifteen months has surfaced certain activities or models that could be especially valuable for accountability and transparency.

These could be applicable to different policy-setting forums, ranging from those at the United Nations to national practice and initiatives led by nongovernmental stakeholders as well as to different actors including states, private cybersecurity providers, contractors and private software manufacturers and distributors. They also range in their level of formality, the degree of costs and penalties imposed, and type of accountability they enforce.
Much has been written and said about attribution in relation to accountability. Political attribution statements, building off technical and legal analysis, will continue to be an important aspect of accountability and deterrence efforts, as are technical characterizations, information-sharing mechanisms or repositories about capabilities, threat actors and groups, tactics, and attributive techniques and tools. But more can be done to increase their impact. Many agree that “naming and shaming” has not been sufficient to deter malicious cyber activity.

- While advances have been made in the rapidity and quality of attribution methods, they can still be improved upon including through better consistency, predictability, and uniformity.

- The possibility of establishing a UN or other multilateral mechanism to aid in attribution has already been explored and largely dismissed as too challenging to create and maintain, although some see value in continuing to explore options of this nature. As attribution capabilities continue to improve, there is merit in revisiting this proposal or approach.

- Leveraging official public political attribution (OPPAs) as a diplomatic tool, through responsible, professional, and verifiable attribution, and mechanisms to negotiate retaliatory measures, can help resolve disputes.
There is a need for building capacity to understand technical attribution reports, and/or to issue or join with political attribution statements.

**Cyber sanctions** did not surface often or explicitly in the research process, which is itself an interesting finding. Yet they are increasingly a companion to attribution statements amongst the small but growing number of countries and regional with relevant policies and are one of the few accountability ‘sticks’ employed to deter malicious cyber activity.

While a new universal legal instrument in this area seems unlikely due to geopolitics and undesirable due to the diverse issues it would need to encompass, a framework convention could be an ideal model for addressing the malicious use of ICT, should the context change. Framework conventions are premised on an initial agreement and then are built out with protocols that focus on related challenges or sub-issues, which states are invited to adopt and ratify as the protocols are developed. The United Nations Framework Convention on Climate Change, the Vienna Convention, and the Convention on Certain Conventional Weapons are examples.

Politically binding agreements—including declarations and codes of conduct—will continue to be useful for signaling about what is and what is not acceptable behavior, and for designing responses that respond to particular challenges or context. In the current geopolitical context, politically binding agreements may offer the best way forward short of new binding law. Often, signatories and supporters of political declarations or political instruments work together to outline practical actions to operationalize and enforce the commitments they have signed up to, and help to generate communities of practice. The Programme of Action (PoA) to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (as well as other UN PoAs) and the Montreux Document on Private Military and Security Companies are examples.

Within the basket of politically binding agreements are regulatory framework(s) on peacetime and dual use cyber/ICT focused on restricting use and activity (development, transfer, etc.) These could be accompanied by moratoria or pledges at the unilateral/bilateral level, or among likeminded actors.

What constitutes an appropriate and lawful countermeasure in the cyber context is a complex topic worthy of further discussion and analysis. Cyber countermeasures are typically framed or conceived of in ways that reinforce traditional understandings of deterrence and negative accountability, in which the potential for retaliatory cyber activity from an injured state deters an adversary from ‘attacking’.

Yet, the effectiveness of countermeasures in deterring malicious offensive cyber operations is unclear. Understood differently, our research highlights that there are a range of policy and diplomatic responses that an injured state or a third party may employ as a countermeasure in response to an ‘attack’ including attribution, sanctions, or retorsion. Such countermeasures—even if not often seen as such—offer the potential to improve accountability while also demonstrating voluntary restraint and compliance with international law, and reduce the potential for escalation.
Peer review mechanisms have been largely underexplored in cyber security and cybercrime but could be valuable for assessing the implementation of commitments, such progress on norms, rules and principles of responsible state behavior. They might also be used to assess and ensure conformity with international law in, for example, the use and development of so-called offensive cyber capabilities. Through our research process it has been observed that peer review mechanisms tend to have good levels of participation and buy-in, and the “state to state” format of the Universal Periodic Review, as one example, is appealing to many Member States. There is growing interest within the UN system in developing a peer review process for different agencies or issue areas (i.e. the World Health Organization). Yet, it is important to assess what the impact of the reviews has been to change or improve policy and practice and if there are other lessons learned, such as for stakeholder participation, that would be valuable for potential cyber peer review.

Better leverage existing accountability mechanisms and relevant fora. The cyber community is not starting from scratch, and there are many existing mechanisms, networks, and practices that contribute to accountability, even if they are not always described or viewed as such. These exist at national, regional, and international levels and can include, inter alia: national cyber security strategies; relevant national legislation; national processes for attribution; information-sharing practices and forums that foster trust, including across and within global regions; private sector public reporting; existing cyber confidence-building measures (CCBMs), points of contact directories; initiatives such as the ITU’s Global Cybersecurity Index; and UN-level initiatives such as the National Survey of Implementation.

Yet, some of these can be improved upon or better enforced—for example, can more be done through parliamentary or legislative oversight of national cyber security strategies? Would triangulating cyber accountability goals into existing regional and national development indicators, or commitments under non-cyber frameworks aid in accountability? Could introducing new measurement tools, such as matrices or national reporting, support operationalization of the UN cyber norms in order to identify needs and gaps? Should the UN Security Council be a stronger voice for cyber accountability?

Activities that provide clarity about the applicability of international law and states’ interpretation legal applicability to their use of ICTs will improve the prospects of the law being upheld and adhered to, which should form the basis of all accountability efforts.

Promoting vulnerability disclosures at every level, might ensure that smaller firms have the capacity to detect and report intrusions without being penalized for conformity.

There are many existing toeholds within the human rights community and international human rights law (IHRL) that can also be leveraged to enhance accountability, particularly with respect to ensuring respect for IHRL in cybersecurity and cybercrime law and policy, and to prevent harm or support those negatively impacted. For example, UN Charter and Treaty-Based organs should continue urging states to prioritize cybersecurity and protect critical rights. Individual case petition mechanisms when human rights violations take place in the cyberspace at the national level can provide a second avenue of justice when domestic judicial institutions fail to adequately respond to human rights violations.
• As noted in the Findings, **enhanced cross domain governance** could aid in accountability and deterrence. Possible suggestions from our research include:

  o Updating the UNSCR 1540 Matrices to account for ICT-related threats to nonproliferation.

  o Better leveraging the Montreux Document and ICoCA to address so-called cyber mercenaries, or the use of ICT by private security contractors.

  o Consideration of cybersecurity risks and threats within outer space security policies and law.

  o There is scope to better integrate concerns about cyber security and cybercrime within existing human rights peer review mechanisms such as the UPR.

  o Ongoing work to update Wassenaar Arrangement control lists, with due involvement of relevant technology experts and communities.

• There are unique risks that some **nongovernmental stakeholders** face because of surveillance operations and spyware yet much available evidence that supports accountability against spyware and other intrusive capabilities has emerged from the work of open-source counterintelligence researchers, rather than regulation. Accountability efforts must therefore include consistent support for the monitoring and reporting initiatives of civil society, industry, and other nongovernmental stakeholders as well as protections and safeguards for open-source researchers and counterintelligence specialists, journalists, activists, and whistleblowers.

  o Given the differentiated cyber risks that marginalized groups and individuals face, support for research and documentation in this area is vital for accountability and ensuring accountability.

• **Market mechanisms** such as insurance, credit ratings, product/service security ratings and liability adjustments, as well as tax adjustments and grants, are currently relatively untapped incentives that can play a pivotal role in promoting accountability for securing cyberspace. Market incentives to promote cybersecurity would help build a case that shifts the perception of security from a burdensome requirement or regulation to a value-added effort. One market incentive that could benefit from more coordinated support and integration into policy discussions is insurance, with that industry’s potential to affect cybersecurity going beyond just insurers adjusting policies as underwriters develop clearer understandings of risks. These incentives can create an ecosystem in which cybersecurity becomes a strategic advantage for corporate success.

  o Promoting private sector requirements for consistency in reporting/payouts for cyber incidents, certifications, liability, insurance coverage.

  o Further engagement with re/insurers to develop criteria for coverage and technical definition of systemic risks.

• The interconnected nature of the internet and the rapid evolution of technological change require a **public private partnership collaboration** between governments and private industry. A successful model for accountability in cyberspace should blend the agility and innovation of industry with the
regulatory authority and threat intelligence capabilities of governments. Combined with appropriate market incentives this synergy can create an ecosystem that fosters agreement on risk prioritization, mutual trust, and shared leadership.

Areas for Further Research

In the course of our research, we identified several other non-cyber issue areas and threats that could be worthy of further research. These include:

- Other arms control and nonproliferation instruments:
  - Biological and Toxin Weapons Convention
  - Chemical Weapons Convention
  - Controls over nuclear and radiological materials
  - Electromagnetic spectrum
  - Article 36 Weapons Reviews
- The Open Skies Agreement
- Multiple aspects of the maritime industry, including the Polar Code, the Law of Sea, and how this transnational industry with heavy private sector involvement operates
- Transnational and organized crime, including the Financial Action Taskforce (FATF) peer-review process
- The automobile industry
- The Kimberley Process
- The Nonproliferation Initiative
- To what extent cyber security can be likened to espionage, as an “accepted unacceptable behavior”
- Emerging artificial intelligence (AI) governance structures

Endnotes


Appendix I: UNEP Secretariat and Implementing Agencies

Appendix II: Major Treaties under Outer Space Governance

Across these treaties and agreements, all signatory states assume the liability, accountability, and benefits that come with these terms and conditions. Together they affirm the applicability of the UN Charter and other international law to space activity. Not only do these treaties regulate military space actions, but also non-military, and classified activity in space.

<table>
<thead>
<tr>
<th>Treaty</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Outer Space Treaty of 1967</td>
<td>The OST is a leading document that prohibits national claims of sovereignty, establishment of military bases and weapons, or placement of weapons of mass destruction in orbit or on celestial bodies.</td>
</tr>
<tr>
<td>Rescue and Return Agreement of 1968</td>
<td>The Rescue and Return Agreement recites that states are obligated to return rescued spacecraft personnel and space objects that return to Earth outside the territory of the Launching State.</td>
</tr>
<tr>
<td>1972 Liability Convention</td>
<td>This is an agreement for States to take full responsibility for any damages caused by their space objects</td>
</tr>
<tr>
<td>1976 Registration Convention</td>
<td>Requires States to provide timely data to the United Nations on all objects launched into space. The UN maintains the publicly available Register of Objects Launched into Outer Space to help promote transparency and the peaceful use of space</td>
</tr>
<tr>
<td>The Moon Agreement</td>
<td>Recites that celestial bodies only used for peaceful purposes and cannot be contaminated. Not all States, however, are signatories to this agreement</td>
</tr>
</tbody>
</table>
The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

STIMSON.ORG

© Henry L. Stimson Center