STIMSON

REPORT

Trade & Technology

Cyber Program

Cyber Deterrence Project

Beyond Denial: Toward a Credible Cyber Deterrence Strategy

By James A. Siebens, Author; Allison Pytlak, Author; Kathleen Scoggin, Research Support

October 2025

ABOUT STIMSON

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

Acknowledgments

This project was made possible through the generous support of the Microsoft Corporation. We are grateful to Kathleen Scoggin for her research contributions to this project, and to Brian Finlay, Rachel Stohl, Julian Mueller-Kaler, and the Stimson Center. Special thanks to Talita Dias, John Hering, Louise Marie Hurel, and Teddy Nemeroff for their insightful comments and suggestions, and thanks to all of our colleagues who contributed to the interviews and dialogues associated with this project.

Please Cite this Publication As

James A. Siebens, Allison Pytlak, Kathleen Scoggin, 2025, *Beyond Denial: Toward a Credible Cyber Deterrence Strategy*.
The Stimson Center, Washington D.C., USA.

Contents

Executive Summary 2

Introduction 5

Restoring Deterrence 7

Understanding the Threat Environment: Why we need Cyber Deterrence 10

The Link Between Deterrence and Accountability 13

Types of Deterrence 16

Why "Cyber Deterrence" is Harder 19

Pursuing Deterrence in the Cyber Domain 23

Beyond Denial? Toward a Practical Deterrence Strategy 27

Conclusion 34

Executive Summary

Each year, the global cyber threat landscape becomes more dangerous and complex. Sophisticated cyber threat actors—many backed by powerful nation-states—are rapidly improving their technical sophistication and adaptation while blending criminal and geopolitical objectives in ways that make defenders struggle to keep pace.

Current cybersecurity strategies that focus primarily on defense and resilience as approaches to deterrence are proving inadequate. Yet, and despite longstanding debate over its utility and relevance, deterrence remains a highly relevant concept and worthy objective for cybersecurity and defense policy.

This paper argues that in the current context of ever-increasing cyber threats and harm, there is a need to revisit this debate and identify practical and actionable methods to complement cyber defense and resilience, which alone appear insufficient to stem the tide of cyber threats and threat actors. This paper attempts to move the discussion about cyber deterrence beyond the idea that "denial" is the best approach to deterrence in the cyber domain, and presents the case that greater accountability for irresponsible, unlawful, and unacceptable behavior in cyberspace would contribute to deterrence.

After clarifying the theoretical debate about deterrence in cyberspace, outlining the link to accountability, and situating both concepts in the current cyber threat landscape, this report provides practical guidance for policymakers seeking actionable methods to reduce harmful cyber operations.

Key Points:

Improving cyber defense and resilience remain essential elements of cyber strategy but are not as effective at creating "deterrence by denial" as is often asserted or assumed by policymakers and practitioners. Deterrence requires that actors who consider engaging in prohibited or harmful behaviors are persuaded that doing so will lead to negative consequences that outweigh whatever benefits they may hope to derive. This is aligned with what is understood to be negative accountability. A credible deterrence strategy must include a genuine commitment to clarifying and enforcing "red lines" by threatening and, if necessary, imposing punitive costs in response to violations.

Greater cohesion across national approaches to accountability and deterrence can facilitate greater and more consistent collective action to deter and respond to unacceptable and irresponsible behavior.

Accountability mechanisms can provide transparency around both the "rules of the road" for acceptable and unacceptable behaviors in cyberspace, as well as the means by which unlawful, irresponsible, and unacceptable actions are to be identified, arbitrated, and when appropriate, punished.

Effective cyber deterrence is not primarily a technological challenge but rather is primarily a question of political resolve. As much as private companies can aid with technical attribution and threat

detection, only governments can impose legal and economic sanctions, retaliate diplomatically, or establish international rules of engagement as part of a cyber deterrence strategy.

Recommendations:

- **Enhance Strategic Communication and Signaling:** States should clearly articulate their cyber deterrence strategies through laws, treaties, declaratory policies, and other political commitments—identifying actors, actions, and thresholds of concern—and work to develop shared understandings of "red lines" and response frameworks, generally and within formal multilateral arrangements, to reduce ambiguity and the risk of miscalculation.

- **Establish Common Standards for Attribution and Accountability:** Develop shared evidentiary standards and transparent attribution practices at national, regional, and multilateral levels, clarifying which international laws or norms are violated and ensuring accountability through coordinated political or legal responses. Exercise offensive capabilities responsibility and lawfully.

- **Strengthen Legal and Normative Foundations:** Advance international agreement on definitions and applications of key concepts such as sovereignty, coercion, and use of force in cyberspace. States should regularly publish and update their national interpretations of how international law applies to cyber operations, including perceived thresholds for concepts like "use of force" and "armed attack."

- **Develop Credible and Responsible Consequence Mechanisms:** Ensure deterrence credibility through lawful, proportional responses—including sanctions, indictments, countermeasures, and diplomatic measures—while maintaining commitments not to target civilian infrastructure or enable criminal cyber activity.

- **Deepen International Cooperation and Coalition Building:** Reinforce cooperation within and among alliances (e.g., NATO, EU, ASEAN, OAS) to coordinate responses to cyber threats, share threat intelligence, and uphold collective deterrence through consistent application of norms and law.

- **Advance Global Enforcement and Legal Integration against Cybercrime:** Implement international cybercrime commitments through domestic legislation and judicial cooperation. Support emerging efforts—such as the International Criminal Court (ICC) work on cyber-enabled crimes—to create stronger deterrence through international accountability mechanisms.

- **Invest in Cyber Capacity, Resilience, and Deterrence by Denial:** Expand CERT/CSIRT networks, strengthen critical infrastructure protection, integrate secure-by-design principles, and ensure sustainable funding, workforce development, and cyber hygiene to reduce vulnerabilities and signal strategic resolve.

- **Expand Public–Private Collaboration and Accountability Frameworks:** Promote structured cooperation between governments and private cybersecurity firms on intelligence sharing, active defense, and response coordination. Support industry-led initiatives, such as codes of conduct and industry standards for the provision and use of commercial intrusion tools or ransomware, as rooted in norms of responsible behavior.

Introduction

Each year, the global cyber threat landscape becomes more dangerous and complex. Sophisticated cyber threat actors — many backed by powerful nation-states — are rapidly improving their technical sophistication and adaptation while blending criminal and geopolitical objectives in ways that make defenders struggle to keep pace. The line separating state-sponsored espionage and coercion from sabotage and cybercrime is narrowing. Private individuals, businesses, and the public sector are often exposed to cyber threats without having the resources, technical know-how, or support from national cybersecurity institutions they need to effectively protect themselves and their data.

There has been a long-standing debate about the feasibility of applying traditional concepts of deterrence to the cyber domain. While initially this was a popular approach, especially among academic and policy experts, over time it has become clear that the primary characteristics of cyber operations and capabilities have rendered traditional approaches to deterrence inadequate or inapplicable. The prevailing wisdom has been that a better framework for understanding the cyber domain is "persistent engagement" in an "agreed competition." As such, governments have tended to shift resources toward cyber defense and resilience, as well as offensive cyber capabilities, ostensibly for purposes of proactive defense through intelligence collection, threat monitoring, and disruption.

Yet, in the current context of ever-increasing cyber threats and harm, there is a need to revisit this debate and identify practical and actionable methods to complement cyber defense and resilience, which alone appear insufficient to stem the tide of cyber threats and threat actors. This paper attempts to move the discussion about cyber deterrence beyond the idea that "denial" is the best approach to deterrence in the cyber domain, and presents the case that greater accountability for irresponsible, unlawful, and unacceptable behavior in cyberspace would contribute to deterrence.

Cyber deterrence holds a direct connection to cyber accountability. This is because deterrence relies on the credible threat that a prohibited action will result in defeat, or punishment. In the cyber context, accountability typically refers to obligations by actors (usually states) to refrain from, and to collectively punish, malicious actions that would violate agreed norms and international law by imposing costs and consequences for such violations. In this sense, accountability is intended to deter actors from violating norms, rules, and mutual commitments. Yet, accountability can also be viewed in a positive sense: being answerable for fulfilling an obligation, such as actions or policies that must be enacted and upheld to maintain cyber resilience, or to render assistance to others in addressing cyber incidents, for example. Broader acceptance of a positive accountability lens might offer a complementary direction for deterrence through mechanisms for accountability.

While all malicious cyber behavior is worth discouraging, deterrence requires that would-be offenders expect to be caught and punished, and that the punishment will outweigh whatever benefits they may hope to gain. It would therefore benefit policymakers at either national or multilateral levels to identify the specific behaviors their deterrence efforts are aimed at preventing, and what they are actually willing to do to punish different behaviors as a matter of policy. Greater cohesion across national approaches to

accountability and deterrence can thereby facilitate greater and more consistent collective action to deter and respond to unacceptable and irresponsible behavior.

This paper presents a brief account of the theoretical and practical prerequisites for any strategy intended to create or improve deterrence in cyberspace and offers a modest critique of contemporary skepticism and dismissiveness regarding the potential application of deterrence theory to cyberspace. It does not attempt to thoroughly recount the well-trodden debate over the analogs and limitations of traditional conceptions of deterrence in the cyber domain but rather accepts these as established.[1] Instead, the goal is to clarify the fundamental requirements of any effective deterrence strategy, and more specifically, how to better deter states, corporations, and individuals from conducting malicious cyber campaigns, operations, and actions. It seeks to move beyond deterrence "denialism" by outlining several practical approaches.

The report consists of the following sections. First, it outlines the current state of affairs in cyberspace, underscoring why malicious cyber activity is a threat to be taken seriously and worthy of deterring. The report then breaks down how deterrence is classically understood and offers a modest critique of contemporary skepticism of cyber deterrence. It then outlines how accountability and deterrence are currently being approached in the cyber domain and outlines the linkages between the two concepts. Finally, the report culminates in a series of recommendations for policymakers that attempt to move beyond theoretical frameworks to actionable strategies that can effectively influence adversary behavior, protect critical assets, and establish credible approaches to accountability as part of a deterrence strategy.

This paper is part of the Stimson Center's Cyber Deterrence project, in connection with the Cyber Program's ongoing work on the topic of cyber accountability.[2] Some of the views and accounts of contemporary policy approaches presented in this paper are based on a series of multi-stakeholder Track 2 and Track 1.5 meetings held under the Chatham House Rule[3] in Brussels, Bangkok, and Washington, D.C. during 2025, as well as several informal not-for-attribution interviews with experts and practitioners from the U.S. and Europe. While these discussions were an integral part of the research for this paper, and served as testing grounds for the arguments herein, the analyses and conclusions presented here belong solely to the authors.

Restoring Deterrence

Despite the manifest realities of persistent engagement in the cyber domain,[4] deterrence remains a highly relevant concept and worthy objective for cybersecurity and defense policy.[5] Indeed, the current draft of the 2026 National Defense Authorization Act (NDAA) directs the Secretary of Defense to develop a strategy for credible deterrence against cyberspace attacks, especially those targeting US defense critical infrastructure. The insights and recommendations offered in this report are intended to support the goal of developing a more credible strategy for deterrence in cyberspace.

The quantitative increase and diversity of cyber threats cannot be safely ignored and indicate a growing need for establishing effective approaches to deterrence in cyberspace, if only on the margins. Cyber activities can affect individuals, societies, states, and the international system in a wide variety of ways, from financial and economic harm to the disruption of essential public services, or even the loss of human life. From election interference to espionage, intellectual property theft, and critical infrastructure disruption, cyberattacks[6] and information operations[7] represent significant threats that can be used coercively, disruptively, destructively, and for material or financial gain. These often constitute physical targets inside the sovereign territory of the defending country, with the potential to damage or disrupt.

The consequences of serious cyberattacks can be so severe that they may justify employing the full range of deterrence tools and tactics typically reserved for conventional and strategic national security threats. The ability of cyberattacks to target critical infrastructure and other "rear-area" resources deep inside another sovereign country can make some cyber capabilities potentially "strategic weapons." This in turn makes the cyber domain a "double-edged sword" in international security. It offers significant options for intelligence collection, sabotage, and coercion below the threshold of armed attack, not to mention strategic deterrence and attack. At the same time, it creates mutual vulnerability, presenting an enormous attack surface for foreign adversaries and criminals alike, with the potential for unpredictable harm and risk of escalation.

However, attacks of such severity are not the only types of operations that governments may wish to deter. Lower level malicious cyber operations, attacks, and intrusions are persistent and ubiquitous, indicating the general failure or severe limitations of past efforts to consistently or fully implement cyber deterrence. The disruption and cumulative harm resulting from these more persistent, lower-level malicious cyber activities are clearly costly enough to call for additional concerted thought and effort on ways to deter, limit, and mitigate unlawful, malicious, and irresponsible behavior in cyberspace by state and private actors alike.

The prevailing wisdom among many in the defense community holds that traditional theories of deterrence are inapplicable or impracticable in cyberspace, and that a better framework for understanding the cyber domain is "persistent engagement" in an "agreed competition." In brief, as Michael Fischerkeller and Richard Harknett put it, "Agreement to compete robustly short of armed conflict may be the grand strategic consequence of cyberspace."[8]

As such, governments have tended to shift resources toward both cyber defense and resilience, and offensive cyber capabilities, ostensibly for purposes of proactive defense through intelligence collection, threat monitoring, and disruption. However, it must be appreciated that these same capabilities and related operations are often indistinguishable from capabilities and operations used to create and exploit vulnerabilities for others. This confounding "cyber security dilemma"[9] represents a key challenge for those working to improve deterrence of malicious cyber activities and those seeking to advance multi-domain deterrence, intelligence collection, and defense by leveraging cyber capabilities.

States already view some cyber operations and activities as amounting to uses of force or armed attacks. Moreover, there is already international agreement that relevant international law – international humanitarian law (IHL), or the law of armed conflict (LOAC) – does indeed apply to the conduct of cyber operations by belligerents during an armed conflict.[10] While there is widespread agreement that some actions in cyberspace can equate to a "use of force" or an "armed attack,"[11] there is no clear agreement on how to define or determine when cyberattacks reach those thresholds using transparent scale and effects-based assessments based on empirical and agreed-upon tests. Instead, they are assessed by the subjective harms resulting from the attack determined by targeted states.[12] This lack of an agreed-upon threshold for an armed attack delivered by cyber capabilities represents another major challenge for policymakers.

In 2017, President Trump ordered the development of "strategic options for deterring adversaries and better protecting the American people from cyber threats."[13] A key recommendation from the resulting report[14] was: "To achieve the stability necessary to maintain and promote the U.S. vision for an "open, interoperable, reliable, and secure internet," the United States and its likeminded partners must be able to deter destabilizing state conduct in cyberspace." The report also recommended two strategic objectives, or "desired end states of U.S. deterrence efforts":

- "A continued absence of cyber attacks that constitute a use of force against the United States, its partners, and allies; and
- A significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force."

However, the vast majority of malicious actions in cyberspace are not even close to the equivalent of armed attacks or uses of force, but rather are designed to cause disruption, create financial gain, or collect sensitive or proprietary information without triggering retaliation or escalation. Deterrence is more difficult – and under-theorized – at these lower levels of interaction, below the level we would think of as a use of force or armed attack. This is partly explained by a desire to avoid international escalation over common practices. For example, while it is generally understood that international espionage is a widespread, even normal, behavior of states, it is also something that states seek to prevent and is thus usually classified as a domestic crime. Many governments understand espionage as a common feature of statecraft, and yet it is also considered a violation of sovereignty that states typically go to great lengths to prevent whenever possible.[15] States therefore typically avoid imposing the kinds of escalatory punishments on others that might provide more effective deterrence because they don't want to be subjected to similarly harsh penalties for their own espionage.

Here it is important to appreciate that the concept of deterrence was originally developed for, and is most commonly applied by, governments in the context of law enforcement. In this context, deterrence is less of an "end state" to be achieved, but rather a strategic objective that requires persistent effort on an ongoing basis to apply defined rules and enforce them through defined processes. However, an underlying challenge is a lack of common understanding and varied interpretation of how states understand their obligations under international law as applying to their use of ICTs, and the absence of a centralized enforcement mechanism.

Understanding the Threat Environment: Why we need Cyber Deterrence

In a world of bloodshed and extreme physical violence, it can be challenging to view cyber and digital security as being the kinds of threats that countries fight wars over, the way that bombs, drones, and blockades are. Yet, cyber operations are increasingly destabilizing international and national peace and security by normalizing attacks on civilian infrastructure, undermining democratic processes and sovereignty, exposing sensitive information, and creating dangerous escalation dynamics where threat actors can inflict significant harm while maintaining plausible deniability. Essential infrastructure, institutions, and public services cannot defend themselves through resilience alone against persistent, sophisticated attacks. Deterrence measures aim to reduce the frequency and intensity of these threats, complementing defensive measures.

Individuals, societies, organizations, businesses, and all levels of government are affected. Some activities emanate from criminal actors purely for financial gain. Others are directly or indirectly linked to governments or political movements and intend to advance political, military, or foreign policy objectives.[16] One study estimates that states now routinely deploy cyber operations, disinformation campaigns, intelligence operations, and infrastructure sabotage as standard tools of competition in ways that remain below the threshold of open warfare.[17] State-linked cyber operations have grown significantly over the past two decades, and the same study estimates that more than 130 countries and territories have experienced some form of cyber disruption. More than 100 have been targeted by foreign influence operations, and around half have seen attacks on their physical infrastructure.[18]

The strategic use of cyber capabilities by both state and non-state actors has become a common feature of both international competition and conflict. Current conflicts in Ukraine, the Middle East, and Sudan, and the recent India-Pakistan crisis, show how states are using cyber capabilities, including influence operations, to pursue their strategic goals. These have at times also deliberately targeted allies of warring parties[19] or have had inadvertent spillover effects into third party states.[20] Outside of conflict, nation-states increasingly utilize cyber capabilities to pursue strategic advantage, from espionage (e.g., Salt Typhoon) to potential sabotage (e.g., Volt Typhoon),[21] with some operations or campaigns pursuing long-term influence objectives,[22] and others presumably pursuing strategic deterrence.[23] Efforts like Salt Typhoon, or other foreign-sponsored efforts to exploit vulnerabilities in U.S. critical infrastructure,[24] can provide perpetrators with significant informational and intelligence advantages, and efforts like Volt Typhoon can in some cases put vital public services and assets at risk. Such operations can therefore demonstrate the credibility and coercive potential of offensive cyber capabilities, including through prepositioning.[25] Prepositioning can constitute an implicit credible threat of disruptive or destructive cyberattacks with

strategic effects, and thus provides a potential approach to using cyber capabilities for purposes of creating or reinforcing strategic deterrence. At the same time, this is exactly the type of coercive threat that states may be most concerned with preventing through deterrence, precisely because prepositioning can provide an implicit and latent threat to impose costs and consequences contingent on the behavior of the actor whose systems have been compromised.

Whether stemming from ransomware, hack and leak operations, man-in-the-middle attacks or other forms of malware including intrusive capabilities (spyware), cyber operations have real effects on the provision of government services (e.g., Costa Rica 2022; Albania 2022);[26] critical industries and infrastructure such as healthcare (e.g., WannaCry 2017; Medibank 2022)[27] and supply chains (e.g., Colonial Pipeline 2021).[28] Many operations expose personal data in ways that are damaging to individuals or public officials (e.g., OPM Hack 2015; SolarWinds 2021),[29] or even at-risk populations (e.g., ICRC breach 2022).[30]

Yet not all cyber operations capture major headlines or amount to serious harm but they are occurring on a constant basis and with potent effects. Consider that Microsoft reportedly blocks 600 million cyberattacks per day targeting its customers and processes 78 trillion daily security signals.[31] Google reports blocking more than 100 million phishing attempts per day, and their TAG services track over 270 government-backed threat actors.[32] And Cloudflare blocked 21.3 million DDoS attacks in 2024, averaging 4,870 attacks per hour.[33]

An important dimension of the current threat landscape pertains to democratic processes and non-intervention. The world has experienced a marked increase in the number of cyber operations since January 2024,[34] not least in connection with the high number of national elections held globally that year.[35] Cyber operations that appear aimed at manipulating or disrupting a country's democratic processes are likely to be viewed as especially threatening, as such campaigns and operations may be readily interpreted as violations of sovereignty or the principle of non-intervention.[36] These cyber operations have included both the potential for direct attacks on electoral infrastructure and also related influence operations such as mis- or disinformation campaigns, which are cyber-enabled. Questions about the application of international law in cyberspace, how it relates to influence operations, and the implications of the international legal principles of national sovereignty and non-intervention for cyber operations, remain topics of debate in the international legal community, and election interference continues largely undeterred.[37]

Artificial intelligence (AI) is also rapidly becoming a more significant factor in aiding both defenders and attackers, the net effects of which remain unclear. While its use is still maturing, threat actors are experimenting with AI-generated deepfakes, including videos, images, and audio, in addition to using AI-assisted coding and AI-powered hacking tools. For example, China has deployed generative AI for influence operations and narrative-building, Russia has embraced synthetic media for political interference, and Iran and North Korea have been exploring AI-driven social engineering (e.g., spear phishing) operations.[38] This has contributed to the proliferation of threats, the sheer volume of which has overwhelmed many sectors, particularly information technology (IT), education, and government. At the same time, AI-supported advancements in cybersecurity tools and practices are aiding in cyber defense, although do not appear to have yet led to a significant reduction in the quantity of such threats.

Advancements in cyber defenses have not translated into deterring malicious cyber activity; the overall toll of malicious cyber activities, including fraud and intellectual property theft, remains massive, driven by the creativity and persistence of malicious actors exploiting every available vulnerability. Faced with a problem of both scale and technical sophistication, with threats often generated by foreign actors, victims and stakeholders are looking to their governments with increasing urgency to better protect them by developing better approaches to deterrence in cyberspace.

The Link Between Deterrence and Accountability

In recent years, there have been a greater number of efforts to impose consequences for malicious cyber activity through cyber-related sanctions, attributions, and responsive action. Despite these efforts, threat actors operate with relative impunity. This speaks to the accountability gap in cyber — even when cyber operations and activities clearly run counter to agreed norms or principles of international law, the responses to such violations vary widely and are applied inconsistently. A complicating factor is that policymakers often aren't willing to bear the costs of imposing consequences that make a difference because the benefits of cyber deterrence do not, or rarely, outweigh the costs.

Given an ever-expanding level of cyber activity, and the clear implications for global and national peace and security, advancements in cyber defenses have not translated into deterring such attacks at their source. Cyber defense and resilience will always be important components of deterrence, but other means need to be considered too — including the imposition of accountability mechanisms and tools. The overall toll of malicious cyber activities remains significant, driven by the creativity and persistence of malicious actors exploiting every available vulnerability and the relative lack of accountability for such behaviors.

Deterrence is necessary because the current lack of consequences creates a dangerous structure where states and other threat actors face minimal costs for inflicting significant harm through cyber operations. Without deterrent measures, this behavior will likely continue escalating as it becomes normalized, leaving critical systems, individuals, and institutions perpetually vulnerable. Deterrence is essential to shift the risk-benefit calculation in ways that prevent harmful action and halt the erosion of international law and norms, and other guardrails. Effective deterrence can play a role in closing the accountability gap that currently shields aggressors from meaningful consequences.

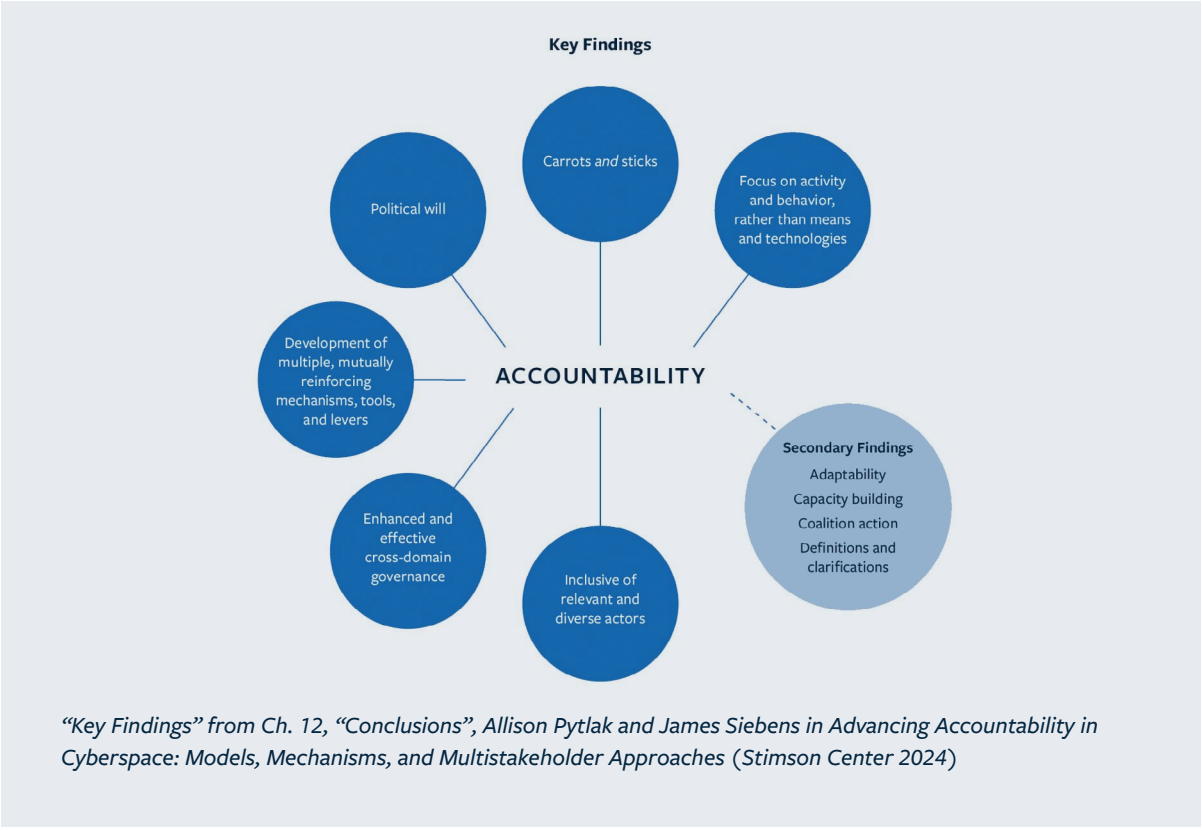
In 2024, the Stimson Center published a report, Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches.[39] The report's introduction outlined a key premise for Stimson's work on accountability; namely, that stronger or more robust accountability mechanisms would "...improve deterrence of malicious cyber activities."[40]

The term "deterrence" by itself can have a very negative — and even frightening — connotation for many people, especially those from outside the field of international security, who may tend to conflate it with, or reduce it to, the analogy of "strategic nuclear deterrence." This invokes the threat of mutually assured destruction and the idea of preventing a nuclear war by convincing nuclear powers that a nuclear war cannot be won and must never be fought. While this is one meaning, or use case, of the concept

of deterrence, it is far from the only meaning. Deterrence is also sometimes reduced to the concept of "general deterrence," which is a strategy of "long-term efforts to prevent any hostile actions," as opposed to "immediate deterrence," which is intended to address situations of clear and present, even urgent, threats.[41]

Both of these common misapprehensions about deterrence should remind practitioners to reflect on, and center, a single guiding question when considering deterrence strategies: "What behavior(s) are we seeking to deter?" If the answer is "everything," or "we don't know," then failure is practically a foregone conclusion.

Properly understood, deterrence is nothing more than a concerted effort to convince others not to do things we don't want them to do. Deterrence is fundamentally about social communication. Indeed, the French word for deterrence is simply dissuasion — this is perhaps the better way to think of deterrence because it prompts us to consider that any measures taken to dissuade another actor from taking a certain course of action can be part of a strategy of deterrence, including things like incentives, accommodations, and assurances (i.e., carrots) that provide positive complements and inducements to the stated or implicit threat of consequences or costs (i.e., sticks). This is part of the reason it is important to understand the concepts of deterrence and accountability as inherently interrelated and mutually supportive.[42] In brief, accountability can create deterrence, and vice versa. Positive accountability creates shared understandings of responsible and acceptable behaviors, and negative accountability promises to impose costs or consequences on perpetrators if deterrence fails.



"Key Findings" from Ch. 12, "Conclusions", Allison Pytlak and James Siebens in Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches (Stimson Center 2024)

Accountability also comes in both positive and negative forms, as outlined in our 2024 report on the topic. Asking people, organizations, companies, and governments to take actions to demonstrate their commitment to a set of rules or norms, and to help build confidence that they intend to comply with the rules, can provide a kind of positive accountability. Negative accountability is essentially the enforcement of norms and rules by enacting penalties and imposing costs for violations of those norms and rules. Penalties can be purely social (reputational), or economic, or they can be physical — the important thing for deterrence is that the penalty is sufficient to decisively outweigh the prospective benefits of "breaking the rules," *specifically from the perspective of the actor(s) being deterred*.

As also outlined in our 2024 report, broader acceptance of a positive accountability lens might offer a promising complement for deterrence by leveraging and combining different mechanisms for accountability, both negative and positive. In this sense, the efforts of states to more explicitly define responsible state behavior through the UN Groups of Governmental Experts (GGEs) and Open-ended Working Groups (OEWGs) on information and communications technology (ICT) since 2004 have advanced the goal of deterring malicious behavior in cyberspace simply by building international agreements and mutual political commitments around the normative responsibilities that states have to one another, for example in providing assistance to victims and preventing their own territories from being used for malicious cyber operations against other states.[43] These commitments build on the universal recognition that international law applies in cyberspace, which further contributes to deterrence through existing and potential mechanisms for enforcing international law.

By building acceptance of the "rules of the road" through existing legal obligations and voluntary commitments that actors can voluntarily abide by, the multi-stakeholder international community can develop more formal and binding agreements, such as treaties and political commitments, with corresponding incentive structures to define and enforce prohibitions on specific types of behavior in cyberspace that should be considered unacceptable. As Dr. Chris Ford explained in 2020, while serving as Assistant Secretary of State for International Security and Nonproliferation, "For such understandings of what constitutes responsible behavior are also critical to understanding what behavior is irresponsible — and that, in turn, opens up possibilities for efforts to make such irresponsibility increasingly unattractive to its would-be perpetrators. This is the burgeoning arena of cyberspace deterrence."[44]

Types of Deterrence

To understand deterrence in the cyber domain, it can be helpful to revisit core concepts of deterrence theory.

Deterrence is generally discussed in terms of two main forms, or theories of deterrence, both of which are closely related to the idea of rationality, and more specifically, "risk aversion" and "cost sensitivity." The first approach to deterrence is called "deterrence by denial" — this is the idea that a threat actor can be deterred from acting if they are persuaded that they likely won't be able to achieve their objective(s) and would thus be wasting valuable resources in the effort. They are thought to be deterred by the prospect of a costly failure — squandered resources with little or no benefit to show for it.

The second approach to deterrence is called "deterrence by punishment" — the threat of consequences in response to some defined or perceived offense. This approach is intended to affect the cost/benefit calculation of the target of deterrence, to persuade them that the costs they would incur as a result of pursuing their preferred course of action would negate or outweigh whatever benefit(s) they could anticipate gaining from it. While their effort might succeed in achieving its immediate objective (e.g., using cyber capabilities to disrupt internet connectivity), in the end, doing so would bring them more harm than benefit because of the costs/penalties that would be imposed on them as a result.

Both of these approaches to deterrence assume that threat actors are basically rational and will decide to act or refrain from acting based on a calculation of the associated costs and benefits. Thus, by persuading potential attackers that their efforts will fail to deliver the intended results, and/or by increasing the anticipated costs of pursuing a course of action beyond what they would consider acceptable, one can dissuade (deter) potential attackers from carrying out their preferred course of action. These are not the only forms of deterrence, but they are the two most discussed.

A third approach to deterrence is "deterrence by detection," which is arguably embedded in, and a prerequisite to, the concept of deterrence by punishment. In brief, this is the idea that one of the surest ways to dissuade actors from doing bad things is to convince them that they will be caught and exposed, which forces them to consider the risk of being prosecuted or otherwise punished, and to expect that, at a minimum, their actions will result in reputational harm and related political and economic costs. While detection in the absence of a credible threat of punishment may make for relatively weak deterrence, the fear of potentially facing unknown consequences after being caught in the act may function as a psychological deterrent. This is in line with the prevailing assumptions of those favoring

greater ambiguity of thresholds and deterrence threats, who argue that uncertainty about the specific triggers for retaliation, and about the specific forms of that retaliation, is beneficial for deterrence.

In order for deterrence to work, there must be a shared understanding (or at least similar assumptions) about what behaviors are acceptable or unacceptable (often analogized to a "red line"[45] for deterrence, or "rules of the road" for norms and accountability), and there must be an expectation that unacceptable actions will be met with consequences or defeated outright — a "threat" of punishment or denial. Again, deterrence is made possible by the communication of future costs or consequences through explicit or implicit threats to prevent, defeat, or punish the pursuit of unacceptable or forbidden actions.

Under any approach to deterrence, the implicit or explicit threat of defeat or punishment would only be effective if 1) the deterrer actually has the capabilities necessary to carry out the punishment they are threatening (or at least the target of deterrence believes they do), and 2) they actually have the will to do so (or at least the target of deterrence believes they do). It is therefore essential for the deterrer to make clear what issues it views as important, or what actions would provoke a response, possibly in the form of retaliation or escalation. Thus, any given deterrence effort requires "communication" of interests and intentions, as well as an understanding of both sides' "credibility" and "resolve" around the specific issue(s) involved.[46]

Credibility is the ability and propensity to carry out the intended (or threatened) action, either to prevent or punish prohibited behaviors. In essence, if the threat actor contemplating the prohibited action is incapable of carrying it out in the first place, it does not need to be deterred; and if the side seeking to prevent the course of action cannot or will not follow through on its threats, it cannot reasonably hope to deter. Likewise, if either side is perceived as lacking the political resolve to carry out an action or threat, its commitment can be said to lack credibility. Because the limitations on credibility may emanate from technological, logistical, or political challenges, they may sometimes be directly related to resolve, and sometimes not.

Resolve is the measure of commitment to a particular cause. The idea that one side must be deterred rests on the premise that they would otherwise prefer to take the forbidden action and must be dissuaded from doing so. If they have no practical intention of taking the action, then they do not need to be deterred. On the other hand, if they are strongly committed to a course of action, deterrence can become nearly impossible. The deterrer also needs to communicate its own resolve to prevent or punish the action by carrying out its threats, which may predictably involve costly escalation. As set out in a recent article by Anne Neuberger, "True deterrence requires the capacity to continuously undermine an adversary's capabilities and prepare to impose unacceptable costs."[47]

These theoretical foundations are a prerequisite to any serious consideration of how to craft a strategy to improve deterrence of malicious cyber activities. Deterrence can only be achieved by understanding the cost-benefit calculations of different actors, communicating threshold conditions (i.e., "red lines"), and committing to uphold those conditions by taking measures to impose unacceptable costs if and when the declared or clearly implied thresholds are crossed.

Why "Cyber Deterrence" is Harder

Despite the above efforts, and for a variety of reasons, malicious cyber activities have proven especially difficult to fully deter.

Mixed Signals

The first and most obvious reason why the prevailing approach has led to "agreed competition" and contexts of "persistent engagement" rather than deterrence — and why it cannot be reasonably expected to create deterrence — is the degree of ambiguity over what behaviors different states might be seeking to deter. As explained above, in order for deterrence to work, there must be a shared understanding (or at least similar assumptions) about what behaviors are acceptable or unacceptable (a "red line," or "rules or the road"), and there must be an expectation that unacceptable actions will be met with consequences or defeated outright — a "credible threat" of punishment or denial.

States have agreed since 2013 that international law applies to their conduct in cyberspace and use of ICTs and in 2015 further set out non-binding norms to guide their behavior.[48] This includes the UN Charter, which prohibits the threat or use of force, except in cases of self-defense.[49] The "Articles on the Responsibility of States for Internationally Wrongful Acts," or "Articles of State Responsibility" (ASR) is an important part of customary international law, although certain provisions remain contested. It clarifies that states are responsible for breaches of their international obligations carried out by any "person or group of persons…acting on the instructions of, or under the direction or control of, that State."[50] The International Court of Justice has also upheld the principle of due diligence, and the legal obligation it creates for states under customary international law not to knowingly allow their territory to be used to conduct internationally wrongful acts against other states.[51]

It therefore follows that international law forms the agreed baseline and standard for assessing what is and what is not acceptable cyber activity by both nation-states and the private actors under their jurisdictions. The ambiguity lies in questions about "how does international law apply?" This is why around three dozen countries, the European Union, and the African Union, have all published their national or common understandings about how they interpret international law to cyber conduct. The Association of Southeast Asian Nations' (ASEAN) endorsement of the UN Cyber Norms as a regional bloc and its publication of a checklist for implementing those norms give further credence to the validity of behavioral norms as another element of an agreed baseline, in addition to international law.[52] In the area of cybercrime, the

Budapest Convention and recently adopted UN Convention against Cybercrime help to delineate even further what behaviors are unacceptable and illegal for individuals.[53]

However, and as our consultations confirmed, even at the high end of the cyber threat spectrum, states and international organizations have generally avoided publicly specifying what types of actions would be considered armed attacks that would justify (let alone trigger) responses in self-defense, sometimes purporting that this very ambiguity somehow contributes to deterrence. This preference for "strategic ambiguity" relies on assumptions about adversaries' assumptions about where undeclared red lines might exist and thus promotes a "groping" approach to cyber operations as adversaries probe the limits of both their own capabilities and the threat tolerances and responses of their targets. There has also been a shift away from responding to one-off cyber incidents, accompanied by threat analysis placing greater emphasis on the cumulative impacts of longer-running cyber campaigns and operations.[54]

Given the lack of centralized law enforcement in the international order, states are left to enforce international law themselves. International courts do not have automatic jurisdiction, and even they cannot really enforce decisions. Countermeasures are one of the few ways to enforce law, but states are often reluctant to use these, or to admit publicly that they are doing so. This is a contributing factor to why deterrence in cyberspace is challenging.

In the absence of declaratory policies about the conditions and thresholds beyond which states would respond with countermeasures, legal action, or other cross-domain forms of retaliation as they would in other cases of armed attack, the predictable dynamic is one of probing until a meaningful response is provoked. Deliberate ambiguity thus represents a core confounding challenge for deterrence across the threat spectrum. Unfortunately, a key motivation for avoiding or abstaining from clear, consistent, and legally binding approaches to defining (un)acceptable behavior in cyberspace may be the very permissiveness of the cyber domain and the lack of accountability afforded to the most capable state actors operating in this context.

Attribution Challenges

The next major challenge is the fact that it is sometimes difficult to determine exactly who is responsible for carrying out particular actions due to the technical sophistication of the malign actor, or the limited technical capabilities of their intended target(s). This is an especially vexing issue for developing countries, which may be more reliant on outside experts from the private sector or even foreign intelligence to make technical attributions. Attributing responsibility for a cyber operation and activity is an important first step to determining response and efforts to prevent further operations by the perpetrator. In cybersecurity, especially when operations affect nation-states, attribution is usually viewed in three forms: technical, legal, and political.

Even when the identity of a malicious cyber actor can be readily identified, it is often also difficult to determine with confidence, let alone certainty, what the motivation of the actor is, and whether they are acting independently or on behalf of, or under the direction or control of, a foreign state. This is significant because

of the different approaches to legal accountability that might be pursued in response to the actions of private hackers or commercial malware firms — such as leveraging international law enforcement cooperation and civil lawsuits — compared to the approaches that might be taken in response to the actions of a foreign government, involving political and economic sanctions, countermeasures, and reciprocal escalation. While challenges abound in either case, it is still important to understand the type of actor one is seeking to deter in order to craft an approach with the best chances of success. If one is unable to determine who is responsible, accountability (and consequently, deterrence) becomes nigh impossible.

Further, 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. A key takeaway from Stimson's consultations is that cyber threats are always factored into broader geopolitical and foreign policy considerations; it may not be worth responding or calling out harmful activity in cases in which doing so would likely have a negative impact on other interests that are considered relatively more important. In the ASEAN region, for example, states may prefer not to make public attributions but to instead pursue quiet diplomacy behind the scenes to express concern and seek resolution of cyber threats, or avoid accusing particular states even when identifying threat actors that might be aligned with or directed by a foreign government.[55]

One of the reasons Stimson has focused on researching accountability mechanisms is because there are hesitations, challenges, and/or unwillingness by those with the capabilities to make high-confidence technical attributions to do so consistently and in a manner that is sufficiently transparent to allow independent evaluation and verification. However, the need for more robust and systematic application of technical attribution of malicious cyber activity is critical for deterrence. Attribution remains essential not only for public accountability but also for enabling credible political and legal responses to malicious, unlawful, and irresponsible cyber actions.[56]

Additionally, 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 harm caused by malicious cyber activities. The development and consistent use of more formal, internationally accepted means of creating accountability for those responsible for malicious, unlawful, and irresponsible cyber actions would meaningfully contribute to deterring those behaviors.

Moreover, efforts to call out unacceptable behavior such as through political attribution statements do not always invoke specific principles of international law, or relevant norms, that are in breach or violation.[57] This fails to reinforce the original baseline, undermining both accountability and deterrence.

Multiple Actors

Cyberspace is an inherently complex domain with multiple stakeholders, including states, intergovernmental organizations, multinational corporations, non-governmental organizations, and even private individuals and groups that operate internationally.

Our consultations have consistently reaffirmed the challenges that come with deterring a wide spectrum of threat actors and considering deterrence in peacetime versus in war. This underscores the importance of having diverse deterrence tools to draw from and strategies that are tailored to the particular concerns and security priorities of each country, company, or organization. There are also conflicting perspectives on if and how deterrence is working to date. For instance, there are — thankfully — fewer incidents and attacks at the high-end of the severity spectrum, which may indicate an acknowledgement that there would be consequences for undertaking such acts. At the same time, there are a greater number of malicious and harmful cyber activities occurring at the lower end of the spectrum, notably criminal activity, but there are also more regulations and restrictions in place. This may mean current deterrence methods are ineffective, or it may indicate that more time and more consistent application of enforcement mechanisms are needed for deterrence to accrue.

Lastly, the word "deterrence" itself has been flagged as problematic, particularly (though not exclusively) in the U.S. context. There are too many psychological associations with "nuclear deterrence" or even conventional deterrence, which can detract from practical efforts to implement the concept of dissuasion or behavioral change, often leading "deterrence" to be dismissed out of hand. In other countries and cultures, deterrence is associated with aggression and war, which makes it an unpopular or unhelpful label. This has contributed somewhat to euphemistic policies and strategies labeled as "active defense," even if they include deterrence as an embedded objective.

Pursuing Deterrence in the Cyber Domain

Cyber deterrence is being pursued through a variety of practical tactics, tools, and approaches, even if formal or specific reference to the term is not always present and is often contested. Most states and private actors have moved away from expecting total prevention of cyber threats and accept that some cyber activity against them will occur, given that it is an environment of "unpeace" and persistent competition. Therefore, many actors rightly seek to minimize the impact of ongoing cyber threats through defense and resilience but also have an interest in minimizing the frequency of harmful or especially risky cyber intrusions and campaigns.

Perhaps the most credible mechanism by which states can set threshold conditions for cross-domain deterrence of malicious cyber activities (leveraging the threat of military intervention or retaliation in or outside of the cyber domain) is through ratifying treaties and enacting domestic laws. These mechanisms publicly and legally commit states to uphold certain rules and red lines and thereby make it impossible for others to transgress without knowingly provoking the threatened response. Formal doctrine and declaratory policy can also provide public signals of resolve about the threshold conditions to be upheld by states. The United States, for example, has historically experimented with the use of declaratory policy to deter malicious cyber activities, although such declarations have tended toward vague, ambiguous, and subjective thresholds, arguably impeding their potential to credibly deter specific types of behavior.[58]

However, rather than focusing on enforcing rules of the road by imposing costs on malicious cyber actors, in recent years, the predominant approach adopted by national governments, public sector agencies, and private and other actors has been conceptualized as cyber "deterrence by denial," notably by building up cyber resilience — being able to restore functionality quickly after disruption — and defense to prevent successful penetration or exploitation from occurring in the first place. By strengthening national or organizational cyber capacity, systems are hardened and made more difficult to access, which, in theory, raises the cost of conducting cyber operations against them and seeks to deny malicious actors the ability to achieve their objectives. This prevailing approach may be changing, however, noting that in 2025 a handful of countries have made pronouncements concerning offensive capabilities or more assertive cyber behavior and response. In May 2025, the UK launched a new Cyber Warfare Command, which, in partnership with British research organization RUSI, is creating a "community of interest" to encourage new thinking about offensive cyber capabilities.[59] In 2025, newly confirmed Director of the Office of the National Cyber Director (ONCD) Sean Cairncross told his confirmation hearing that, "Fundamentally, cyber is the attack vector, but the adversaries executing cyberattacks are human. As such, the United States must disincentivize this type of behavior by increasing the cost and risk for malicious cyber actors

and nation states. Our adversaries present us with strategic dilemmas in this domain — defensive and offensive — and we need to do the same." A commission has also been established to investigate a long-standing proposal for the US military to create a Cyber Force.[60]

Cyber foreign aid and overseas capacity-building are related means to build resilience, and by extension, deterrence. For example, although it has subsequently been rolled back, the U.S. pledged a significant investment in this area in 2024 in order to bolster the technical capabilities of both allies and "consequential middle-ground states," building on prior experiences with aid to countries like Albania and Costa Rica in the wake of major incidents.[61] Canada has made a significant investment in strengthening cyber engagement and diplomacy in in the Indo-Pacific, including to strengthen cyber defense/interoperability with regional partners.[62]

At the pointier end of the stick, publicly declared national cybersecurity and cyber defense strategies to bear on the challenges of pro-/active cyber defense, which, alongside or in combination with public revelations or demonstrations of so-called "offensive cyber capabilities," can have a deterrent effect. Exact terminologies and framings vary from country to country, but a growing number of states are open about their capabilities and postures and have even published about the conditions for use or approval. Some, like France, keep offensive capabilities distinct from defensive capabilities and describe clear controls over their use; others, like the U.S. and the United Kingdom（UK）, have more integrated approaches involving their intelligence communities. Japan[63] and South Korea[64] are the most recent countries to declare proactive and active cyber defense postures, respectively, with South Korea's as part of ongoing cyber cooperation with the U.S. Such capabilities are a means to pursue broader objectives, including signaling and deterrence. For example, the China-linked Volt Typhoon intrusions into U.S. critical infrastructure may have been intended to dissuade U.S. political leaders from supporting Taiwan in the event of a future conflict.[65]

Nonetheless, there is an enduring need to better define the conditions under which any variety of cross-domain responses can and should be employed in order to render the threat of a decisive punishment, and especially a collective response, to malicious cyber activities more credible internationally. One of the clearest examples of a more integrated approach to deterrence comes from NATO and its iterative policies on cyber defense, based on its focus on both deterrence and defense. Allies have agreed that the nature of cyberspace requires a comprehensive approach through unity of effort at the political, military, and technical levels. They have also recognized that significant malicious cyber activities can have immediate or cumulative effects that would justify considering them as an "armed attack," which could lead the victim of such cyberattacks to invoke Article 5 of the North Atlantic Treaty on collective defense.

However, in the absence of specific criteria for determining an "armed attack," the question of whether or not a particular action or campaign justifies a collective response will continue to be made on a subjective case-by-case basis. While champions of ambiguity might argue that this lack of clarity creates greater room for maneuver and increases room for doubt in the minds of potential attackers, it must also be considered that such ambiguity does little to deter any specific types of actions that some governments may wish to categorically prevent whenever possible. Consequently, ambiguity may encourage probing and raise the risk of miscalculation.

There are a variety of options in the cyber accountability toolbox of political, legal, and technical consequences or costs that can offer deterrent value. Diplomatic demarches and economic sanctions are increasingly employed to signal that malicious cyber activity comes with a cost. Australia, the UK, the U.S. and the European Union (EU) are among those with the most extensive legal frameworks for imposing sanctions on individuals and entities involved in malicious cyber activity. The United States, for example, has imposed sanctions on hundreds of individuals and entities since 2015 in response to malicious cyber activities.[66] However, the effectiveness of sanctions can be limited by factors like their scope, lack of robust enforcement, or a lack of clear and consistent application and communication around the purposes for which sanctions are employed.

Public attribution statements, as informed by technical assessment, legal review, and political judgement, seek to "name and shame" as a form of punishment to discourage such behavior in the future. In recent years, attribution statements from states or groups of states, often building on technical information from the private sector, are surging. These have mostly come from Western countries, but recently, more non-Western countries have made public attributions, including China, Iran, Singapore, and Venezuela.[67] The utility of such statements in discouraging future malicious cyber activity remains unclear as countries named in past statements do not appear to have meaningfully curtailed their actions, but such statements are important for indicating what is and what is not acceptable behavior. This can both clarify national positions on cyber attribution and deterrence and reinforce norms of responsible behavior, producing a cumulative effect over time.

Countermeasures in the cyber domain, or other forms of punitive action outside the cyber domain, can be understood and leveraged as components of cyber deterrence. Countermeasures are responses to a breach of international law that would otherwise be unlawful (though they cannot involve the use of force).[68] The more fluid, covert, and fast-moving nature of the cyber environment raises questions about how the conditions for taking countermeasures, under customary international law, apply in the cyber context. In the absence of well-defined thresholds for unlawful use of cyber capabilities, states are often left uncertain about when it may become legally permissible to resort to countermeasures.[69]

States and other actors sometimes work in coalition to discourage and dissuade threat actors and malicious activity through a range of activities and combined effort. The cyber confidence-building measures established by regional organizations such as the Organization of American States (OAS) and the Organization for Security and Cooperation in Europe (OSCE) view those confidence-building measures as contributing to deterrence by increasing cooperation and information sharing on threats.

In the area of cybercrime, the International Counter Ransomware Initiative (CRI) is an example of a collaborative, multi-dimensional, and highly focused effort. It brings together around 70 member countries and entities on the premise that "International partnerships are a force multiplier against ransomware actors and their ecosystem — [partnerships] strengthen our capability to detect, disrupt, and deter malicious cyber actors that engage in or facilitate ransomware attacks."[70] By working across several pillars, CRI members can undertake coordinated joint disruption actions, share intelligence using a common platform, and assist one another with incident response if their government or critical sectors experience a ransomware attack.[71]

As highlighted in a recent paper by Louise Marie Hurel and Gareth Mott and referenced in some of the above examples, cross-domain deterrence is yet another approach and one that is valuable for going beyond denial and resilience alone.[72] This approach views cyber deterrence not as a standalone challenge, but as one part of a broader state toolkit involving multiple domains and holds that cyberattacks can be deterred through retaliatory threats or actions in other domains. It thus expands the menu of response options beyond cyberspace and enhances the credibility and flexibility of deterrent postures.

The above is not an exhaustive mapping of cyber deterrence efforts to date but is intended to provide an indication of the different ways in which it is currently being pursued.

Beyond Denial? Toward a Practical Deterrence Strategy

Because of these confounding and compounding challenges, many in the defense community seem to have given up on applying the concept of deterrence in cyberspace, having concluded that the cyber domain is so different and unique that deterrence simply does not apply. The inherent complications of the cyber domain, as well as the covert nature of many cyber activities and capabilities, have contributed to widespread rejection of cyber deterrence as a salient and relevant model. However, that strategic view is rapidly changing.

The prevailing approach to deterrence in the cyber domain has been to invest in more effective cyber defense and resilience and to imagine these as contributing to "deterrence by denial" by persuading attackers, over time, that their efforts are ineffective and wasteful such that they eventually decide to give up. By depriving attackers of the ability to achieve their strategic or operational objectives, cyber defense and resilience are thought to fundamentally undercut the attackers' motivation, leading them to pursue other options.[73]

Unfortunately, "deterrence by denial" alone has dubious promise in the cyber domain because of at least two key differences it has from physical battlespace. First, in the physical world, attackers and defenders both experience attrition — they take losses and suffer degradation of their combat power as a result of those losses. Cyber attackers, on the other hand, lose exploits, or certain malicious code might become less effective or ineffective due to improvements or adaptations by defenders. While this might arguably be compared to "attrition," such "losses" in the cyber domain do not significantly increase the marginal cost of new attacks. Secondly, the failure of any particular cyber attack does not render future attacks weaker and less likely to succeed. Indeed, the opposite may be true, as failed attacks provide attackers with valuable information about the defenders' capabilities and potential vulnerabilities without making costly sacrifices of future combat power in the effort.[74]

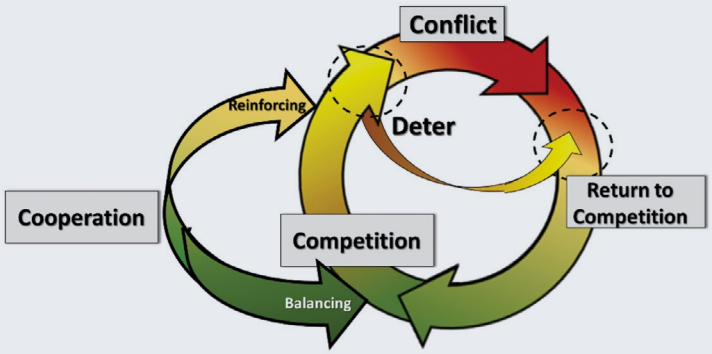
While effective defense is inherently valuable, the deterrent value of the "denial" approach in cyberspace — focusing on defeating and recovering from cyberattacks to persuade attackers of the futility of further attacks in the face of one's defensive capabilities and one's ability to recover from successful attacks — is therefore likely to be quite limited. It depends on the extent to which defensive measures can significantly drive up the marginal costs of offensive measures, which are apparently negligible.

Strategic considerations

To meaningfully deter cyber-attacks and malicious activity, actors need to develop cyber deterrence strategies tailored to their unique capabilities and vulnerabilities in addition to the specific actors and actions they wish to discourage. Whether at a national or a company level, a one-size-fits-all approach is not effective. Hurel and Mott's recent report suggests a two-pronged approach to cyber deterrence strategies when pursued in the context of national or international security.[75] The first prong is to view cyber deterrence as a spectrum of prevention and response measures (from low- to high-impact measures) based on lessons learned from existing cases. The second prong is to position cyber disruptions within a broader non-cyber scale of disruptions, with comparison to what exists for natural disasters, to understand the systemic impact of malicious cyber actions or operations relative to other types of disruption.

Deterrence is only necessary in circumstances where actors have incentives to breach the peace or otherwise violate the interests of others in an intolerable manner. If the status quo in the cyber domain is sustainable — if the legal and financial consequences of cybercrime are bearable and the current boundaries of persistent engagement in an "agreed competition" are tolerable — then there would be no need to contemplate a strategy aimed at deterrence. The fact remains that the costs and strategic risks emanating from the current competition in cyberspace are unacceptably high.

As a first step, any deterrence strategy must determine what it wants to prevent. The objective of a practical cyber deterrence strategy would not be to eliminate all forms of competition in the cyber domain below the threshold of armed conflict, but rather to restrict that competition to genuinely acceptable tolerances. A mixture of competition and cooperation is the inevitable, if not desirable, stasis in all international affairs, not just in the cyber domain. As with other areas of ambiguous, deniable, or irregular competition in the "gray zone" below the threshold of armed conflict, the purpose of a deterrence strategy for the cyber domain would be to reduce, as much as possible, the instance of unacceptable behavior by states and non-state actors in order to support a more sustainable and predictable state of competition in cyberspace. It would be to reduce the risk of interstate escalation to armed conflict resulting from competition by continuously reinforcing the boundaries of acceptable competition, while also working to reduce harms to public and commercial interests from cybercrime and other unacceptable or irresponsible behaviors.



Joint Concept for Integrated Campaigning – Conflict Continuum with Selective Cooperation[76]

As far as state behavior is concerned, international law already applies to the most concerning (potential) behaviors in cyberspace. There is little reason to consider cyber capabilities as fundamentally separate or distinct phenomena from other weapons that produce harmful or disabling effects on people and property. "The novelty of a weapon — any weapon — always baffles statesmen and lawyers, many of whom are perplexed by technological innovation. [A]fter a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles of international law to the novel weapon…".[77]

Core elements and practical actions

An objective of this paper has been to clarify the fundamental requirements of an effective deterrence policy and sketch out approaches that go beyond deterrence by denial alone and align with efforts for cyber accountability. In the following section, we set out five elements, or dimensions, for cyber deterrence and accountability, and within each, suggest relevant actions and considerations.

ELEMENT I: CLEAR COMMUNICATION AND SIGNALING

- Clear communication and signaling are essential components of a credible cyber deterrence posture. The development and implementation of national cybersecurity strategies are an important first step towards clear articulation of a state's position on a range of cyber issues, and often provide the basis for other policies, strategies, and doctrine. While states are at varying stages of national cybersecurity strategy development, few have articulated how these strategies support deterrence objectives or defined the specific behaviors they seek to deter. This creates ambiguity for both adversaries and allies, with unavoidable trade-offs for deterrence.

- One way to begin addressing this gap is to develop deterrence strategies that explicitly identify actors and actions of concern. For countries operating within regional blocs and other alliances, there is value in establishing common positions on "red lines" to guide collective responses, or common standards for evaluating threat severity, etc. Some, like NATO and the EU, are further along in such efforts, while others including the OAS and ASEAN, may wish to consider a similar exercise. While such efforts may not eliminate ambiguity entirely, they can help build internal alignment and cohesion, improve the credibility of deterrence messaging, and reduce the risk of miscalculation.

- In both military and legal contexts, states should also deepen international cooperation to reinforce deterrence of unacceptable behavior by states and non-state actors alike. The goal should be to maintain the agreed competition in cyberspace below the threshold of armed conflict, while deterring more types of unlawful, irresponsible, and unacceptable cyber activities. This means developing compatible, if not coordinated, national positions on what behaviors are truly unacceptable and creating frameworks for coordinated responses in cases of violations of law and norms of responsible behavior, and violations of sovereignty.

ELEMENT II: CREDIBLE CAPABILITIES TO IMPOSE CONSEQUENCES

- Attribution is a key ingredient for cyber deterrence, but it encounters unique challenges in the cyber domain. There are no agreed upon standards of evidence for attribution in international law. Nonetheless, technical capabilities are improving all the time, and an increasing number of states are seemingly growing more comfortable engaging in legal and political attribution of malicious cyber activities. Accused states tend to reject such attributions, however, often alleging that the accusation is politically motivated.

    - As a result, some cybersecurity firms and researchers have called for establishing common levels of transparency and evidentiary standards for attribution, even if disclosing the actual 'evidence' remains impossible or not politically viable. Some have even suggested and scoped out what it would take to establish an independent technical body for cyber attribution.[78]

    - It seems unlikely that the international community will move to establish such an independent body. However, establishing agreed-upon common standards for evidence and prosecution of cyber criminals at national, or even regional, levels would benefit deterrence and improve confidence in such processes, helping to fulfill the accountability potential of attribution. Even when attribution is not linked to a legal process, attribution statements should also specify which international rules and/or domestic laws have been violated, noting the personal and functional immunities of state officials, which impedes their prosecution in domestic courts.

- States seeking to reduce the amount of malicious activity in cyberspace should support the development and application of criminal laws governing the behavior of private actors in cyberspace, as well as relevant evidentiary standards and rules of procedure so that legal evidence of attribution can be presented in a transparent and transferrable format, thus facilitating greater cooperation on law enforcement efforts across national jurisdictions.

- Declaring an offensive capability can signal a response capacity but must be exercised responsibly. Many of what are considered to be "offensive" cyber activities, or active measures for defense, can be considered unlawful or operate in a grey zone; as such, they do not enjoy the same protection and legality as countermeasures, which are reactive as opposed to anticipatory. States could, for example, point to international law and norms in the context of their cyber deterrence strategies and in stating their offensive capabilities by committing to not use those capabilities to target critical infrastructure or interfere with supply chain integrity, or to permit criminal or irresponsible cyber activity within their borders.

- Sanctioning is an increasingly common response to malicious cyber activity, but does it have deterrent value? Greater and more consistent study on the enforcement and impact of cyber-related sanctions would enhance understanding of the efficacy of this approach, including when employed against different types of threat actors (individuals versus multinational corporations, or states) or for different forms of cyber threat (e.g., commercial spyware versus hacking and data theft). Sanctions work best when there is international cooperation on enforcement and compatibility between

global and national commitments. When combined with diplomatic sanctions, such as summons, demarches, or even expulsion, the accountability value of such measures is enhanced, improving the potential contribution to deterrence. However, the use of sanctions requires ongoing study and analysis to assess their impact and effectiveness in practice as an approach to cyber deterrence.

ELEMENT III: UPHOLDING AND ENFORCING INTERNATIONAL LAW AND NORMS

- The most immediately practicable approach to improving deterrence in cyberspace is to improve international agreement on the definitions and practical implications of concepts like "sovereignty," "coercion" (as an element of the principle of non-intervention), "use of force," "armed attack," and "crime" using any workable combination of international treaties, multilateral and national declaratory policies, and domestic laws to match declared red lines with military doctrine and legal regimes.

- Deterrence cannot work if law and norms are poorly enforced. There are agreed standards for what is and is not acceptable state cyber behavior and for cybercrime, as established through existing international law (treaty and customary), agreed behavioral norms, and diverse regional understandings or coalition-led frameworks. Yet the deterrent value of international law and norms has been relatively low to this point because of poor enforcement. There is also a lack of common interpretation of international law and statements of exactly how states are being guided by law in their cyber activities. National interpretations vary in scope and depth and are often unclear in terms of deterrence.

- States should continue to publish, or update, national interpretations of how international law and norms apply to their behavior in cyberspace and should leverage multilateral opportunities to exchange those views. Because these agreements have largely been forged by ministries of foreign affairs, it appears that ministries of defense, intelligence agencies, and technical/information bodies within governments may lack consistent awareness of these multilateral commitments. In some countries, the process of developing national interpretations has generated greater inter-agency or cross-departmental communication.

- In the area of cybercrime, where there is more explicit law to draw from, the challenge of deterrence comes from the transboundary nature of cybercrimes and the jurisdictional limitations of law enforcement. Differences in legal frameworks, data protection regulation, and technical standards, as well as challenges in international cooperation, especially for evidence collection, are exploited by cyber criminals. Implementing international commitments through national legislation enforces and upholds global commitments and provides a foundation for imposing consequences on offenders. States should implement their commitments nationally under relevant cybercrime law and work together through bilateral or multilateral mechanisms to improve information and evidence sharing.

- The recently announced intention of the International Criminal Court to prosecute cyber-enabled crimes, affirming that the Rome Statute's provisions can apply to actions conducted through cyberspace, is a further opportunity to advance accountability and deter future

cybercrimes by states. As highlighted in its Draft Policy on Cyber-enabled Crime under the Rome Statute, "There may be numerous synergies between States' efforts to build capacity to effectively investigate these ordinary cybercrimes — and to enhance State cooperation in that regard — and capacity-building efforts with regard to cyber-enabled international crimes within the Court's jurisdiction, in line with the principle of complementarity."

ELEMENT IV: CAPACITY AND RESILIENCE

- Cyber deterrence by denial remains a valid strategy but comes with inherent limitations, as discussed above. To practically invest in capacity and resilience for deterrence by denial, organizations and governments must take a multi-layered approach. Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) are essential for ensuring that states, international organizations, private companies, and other actors have the capacity and capability to respond rapidly to cyber incidents. These teams should be supported by broader incident response plans tailored to the specific sector and threat landscape. The CSIRTs Network, established under Europe's updated Network and Information Security Directive (NIS2), for example, serves as an example of this broader regional collaboration.[79] The integration of Secure by Design principles into technological development can help to ensure that vulnerabilities are minimized from the outset.

- Resilience, especially for critical infrastructure (CI) and critical information infrastructure (CII), is dependent on adequate funding and resourcing. Ensuring a sufficient flow of financing is both a technical advantage and serves as strategic signaling to other nations. For example, U.S. stakeholders have recently raised concerns about potential reductions in national cyber defense funding and the strategic signal that such reduced funding would send to both adversaries and allies. A strong cyber posture also requires comprehensive risk management frameworks that prioritize threat modeling and mitigation. Finally, workforce development and cyber hygiene are critical: Cultivating skilled professionals and promoting security awareness across all levels of an organization strengthens the human layer of defense, which is often the most vulnerable.

ELEMENT V: INTERNATIONAL AND PUBLIC-PRIVATE COOPERATION

- Deterrence is made stronger when a greater number of actors signal together that a particular action is unacceptable or have agreed to work together on enforcing and upholding relevant law, norms, or cyber security standards, for example. International cooperation through exchanging threat intelligence and coordination on punitive measures can further deter transnational cyber threats. Some of this coordination occurs at the regional or alliance level, through organizations like NATO, ASEAN, the EU, and the OAS. Coalitions of like-minded states can carry significant practical and political weight in reinforcing rules and deterring violations.

- The recently adopted Code of Practice for States on irresponsible use of commercial cyber intrusion capabilities (CCICs) introduces tangible commitments for its signatories and sends a signal that certain uses of these technologies are a concern and deemed "irresponsible," whether for reasons relating to human rights or international peace and security.[80] Governments that have endorsed the Code should

implement the commitments it contains, and those that have not yet done so are encouraged to join. The forthcoming Code of Practice for industry constitutes an important opportunity to further deter misuse of CCICs by introducing reputational consequences, reinforcement of norms, and industry self-regulation or "peer pressure."

- Efforts through the CRI should also be maintained and strengthened. Disrupting active operations, making ransomware less profitable, and creating an environment where the risks of cybercrime outweigh benefits can all have strong deterrent value.

- Outside of interstate cooperation, cooperation between private cybersecurity firms and the public sector, especially in the areas of threat detection and intelligence sharing, will only continue to aid in resilience and defense.

- There is scope for the insurance sector to develop shared policies, frameworks, and terminologies around cyber incidents, which may influence risk behavior and contribute to deterrence.

Conclusion

Malicious cyber activity is a persistent and systemic feature of global security dynamics. Understanding its patterns is essential for developing effective deterrence and response strategies. Bridging the attribution-response gap and reinforcing both legal and political accountability will be crucial to any effort to improve deterrence of malicious cyber activities.

The scale, sophistication, and persistence of today's cyber threats demand a strategic shift. Private industry continues to play a critical role in identifying and defending against attacks. But they cannot, and should not, carry the burden alone. Nor should private companies be encouraged to take unilateral actions to sanction foreign entities without governmental approval. Governments must assume leadership in crafting and enforcing a coherent cyber deterrence framework that is political, legal, economic, and diplomatic in nature. This means establishing rules and norms — such as prohibiting pre-positioning for cyberattacks on critical infrastructure or insisting upon broad international cooperation on law enforcement investigations and prosecutions of cyber criminals — publicly attributing malicious behavior with clarity and consistency, and imposing proportional consequences that may go well beyond the cyber domain. Sanctions and diplomatic pressure must become the new normal for dealing with unlawful, irresponsible, and unacceptable cyber activity. Different types of actors may be more or less receptive to different approaches, from more security-centric tools and approaches to dealing with state actors at the higher end of the threat spectrum, better enforcing criminal and civil laws and regulations, and creating financial and other market incentives and informal or semiformal commitments (for example, agreement to industry best practices) at the lower end of the threat spectrum.

The responsibility to respect and enforce these rules, draw red lines, respond to violations, and impose meaningful costs on perpetrators lies with states and their political leaders. Ultimately, effective cyber deterrence is not primarily a technological challenge; rather, it is primarily a question of political resolve. As much as private companies can provide assistance with technical attribution and threat detection, only governments can impose legal and economic sanctions, retaliate diplomatically, or establish international rules of engagement as part of a cyber deterrence strategy. Without a shift in strategy, states risk allowing the most dangerous threat actors to operate unchecked, with the predictable consequence being the proliferation and intensification of these threats.

What is sorely missing from the equation is the genuine dedication and consistent willingness of political leaders to ensure that state conduct is in accordance with international legal obligations and political commitments. Relatedly, in order for international law and norms to deter unlawful or irresponsible behavior by states and the non-state actors operating within their jurisdictions, there would need to be some means of consistently identifying violations and imposing consequences. This would in turn imply the need for mechanisms designed to enable credible (apolitical) attribution, arbitration, and adjudication of unlawful or wrongful acts across national jurisdictional boundaries.

Endnotes

1 For a thorough account of this debate, see: Stefan Soesanto, Cyber Deterrence Revisited (Maxwell Air Force Base, AL: Air University Press, 2022), https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/CPP_0008_Soesanto_Cyber_Deterrence_Revisited.pdf.

2 Stimson Center, Cyber Deterrence, accessed August 13, 2025, https://www.stimson.org/project/cyber-deterrence/.

3 "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed," Chatham House, accessed August 5, 2025, https://www.chathamhouse.org/about-us/chatham-house-rule.

4 Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, Cyber Persistence Theory: Redefining National Security in Cyberspace (Oxford: Oxford University Press, 2022), https://global.oup.com/academic/product/cyber-persistence-theory-9780197638255?cc=us&lang=en&.

5 Liam Collins and Lionel Beehner, "Thomas Schelling's Theories on Strategy and War Will Live On," Modern War Institute, December 16, 2016, https://mwi.westpoint.edu/thomas-schellings-theories-strategy-war-will-live/.

6 Defined by the National Institute of Standards and Technology, U.S. Department of Commerce, as follows: "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself;" National Institute of Standards and Technology (NIST), Cyber Attack, Computer Security Resource Center (CSRC), accessed August 6, 2025, https://csrc.nist.gov/glossary/term/Cyber_Attack.

7 Defined by the U.S. Department of Defense and the National Institute of Standards and Technology, U.S. Department of Commerce, as follows: "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own;" U.S. Department of Defense, Joint Publication 3-13: Information Operations, 27 November 2012, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf; and National Institute of Standards and Technology (NIST), Information Operations, Computer Security Resource Center Glossary, accessed August 6, 2025, https://csrc.nist.gov/glossary/term/information_operations.

8 Michael P. Fischerkeller and Richard Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," The Cyber Defense Review (Special Edition, 2019), https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.

9 Ben Buchanan, The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations (London: Hurst Publishers, 2017), Ben Buchanan, The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations (London: Hurst Publishers, 2017), https://www.hurstpublishers.com/book/the-cybersecurity-dilemma/.

10 The UN Group of Governmental Experts spent a great deal of time and effort to ensure that IHL is understood to apply to actions in cyberspace, despite the reservations of some States. See: United Nations, Final Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (2019–2021), June 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf; Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace," Just Security, July 12, 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/; It is also important to recognize that the agreed norms of responsible state behavior in cyberspace are broader than IHL, see: Louise Marie Hurel, "The Rocky Road to Cyber Norms at the United Nations," Council on Foreign Relations, September 6, 2022, https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0; United Nations Office for Disarmament Affairs, The UN Norms of Responsible State Behaviour in Cyberspace, March 2022, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

[11] An armed attack is a more serious instance of the use of force, triggering the right to use force in self-defense under Article 51 of the U.N. Charter. See https://cyberlaw.ccdcoe.org/wiki/Use_of_force#Definition; "para 195" https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

[12] Catherine Theohary, Cybersecurity and International Law, Congressional Research Service, updated August 2, 2021, https://sgp.fas.org/crs/natsec/IF11995.pdf; https://www.cambridge.org/us/universitypress/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB

[13] See Sec. 3 (b). https://www.presidency.ucsb.edu/documents/executive-order-13800-strengthening-the-cybersecurity-federal-networks-and-critical#:~:text=States:%202017%20%E2%80%90%202021-,Executive%20Order%-2013800%E2%80%94Strengthening%20the%20Cybersecurity%20of%20Federal%20Networks%20and,as%20an%20executive%20branch%20enterprise.

[14] U.S. Department of State, Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats, Office of the Coordinator for Cyber Issues, May 31, 2018, https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.

[15] Many governments in the Global South consider the interception of communications and cyber espionage to be unlawful under international law. This perspective challenges more permissive interpretations advanced by some Western states. See Darien Pun, "Rethinking Espionage in the Modern Era," Chicago Journal of International Law 18, no. 1 (2018), https://cjil.uchicago.edu/print-archive/rethinking-espionage-modern-era and Katharina Ziolkowski, ed., Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (Tallinn: NATO CCD COE Publications, 2013), 345–47.

[16] Microsoft, How Microsoft Names Threat Actors, Microsoft Learn, updated July 10, 2025, https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming.

[17] Julia Voo and Virpratap Vikram Singh, Power Across Layers of Cyberspace, International Institute for Strategic Studies (IISS), 24 April 2025, https://www.iiss.org/charting-cyberspace/2025/04/power-across-layers-of-cyberspace/.

[18] Ibid.

[19] Canadian Centre for Cyber Security, Cyber Threat Activity Related to the Russian Invasion of Ukraine, Government of Canada, June 22, 2022, https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

[20] Alliance for Securing Democracy, "Russian cyberattack takes down satellite communications in Ukraine," German Marshall Fund of the United States, accessed September 25, 2025, https://securingdemocracy.gmfus.org/incident/russian-cyberattack-takes-down-satellite-communications-in-ukraine/.

[21] Erica Lonergan and Michael Poznansky, "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats," War on the Rocks, February 25, 2025, https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/.

[22] Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in 8th International Conference on Cyber Conflict: Cyber Power, ed. N. Pissanidis, H. Rõigas, and M. Veenendaal (Tallinn: NATO CCD COE Publications, 2016), https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

[23] James A. Siebens and Melanie Sisson, "China's Multi-domain Deterrence of the United States," in China's Use of Armed Coercion: To Win Without Fighting, ed. James A. Siebens (London: Routledge, 2023), https://www.taylorfrancis.com/chapters/edit/10.4324/9781003387770-9/china-multi-domain-deterrence-united-states-james-siebens-melanie-sisson; Nathan Beauchamp-Mustafaga, "Exploring Chinese Thinking on Deterrence in the Not-So-New Space and Cyber Domains," in Modernizing Deterrence: How China Coerces, Compels, and Deters, ed. Roy D. Kamphausen (Seattle: The National Bureau of Asian Research, 2023), https://www.nbr.org/publication/exploring-chinese-thinking-on-deterrence-in-the-not-so-new-space-and-cyber-domains/.

[24] E.g., Sean Lyngaas, "Russia-Linked Hacking Group Claims to Have Targeted Indiana Water Plant," CNN, April 22, 2024, https://www.cnn.com/2024/04/22/politics/russia-linked-hacking-group-targets-indiana-water-plant/index.html.

[25] "Pre-positioning is the process by which computer code is installed on the network or system of a rival state, to allow for future hostile cyber activity if required." See Jann Skingsley, "'Cyber-Rattling': Can 'Pre-Positioning' in Cyberspace Amount to a Threat of the Use of Force under Article 2(4) of the United Nations Charter?" Journal on the Use of Force and International Law 11, no. 1–2 (2024): 50–86. https://doi.org/10.1080/20531702.2024.2413791.

[26] International Cyber Law: Interactive Toolkit, "Costa Rica Ransomware Attack (2022)," NATO Cooperative Cyber Defence Center of Excellence, accessed October 2, 2025, https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022); International Cyber Law: Interactive Toolkit, "Homeland Justice operations against Albania (2022)," NATO Cooperative Cyber Defence Center of Excellence, accessed October 2, https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022).

[27] International Cyber Law: Interactive Toolkit," WannaCry (2017)," NATO Cooperative Cyber Defence Center of Excellence, accessed October 2, 2025, https://cyberlaw.ccdcoe.org/wiki/WannaCry_(2017); Tiffanie Turnbull, "Medibank Hack: Russian Sanctioned over Australia's Worst Data Breach," BBC News, January 23, 2024, https://www.bbc.com/news/world-australia-68064850.

[28] International Cyber Law: Interactive Toolkit," Colonial Pipeline ransomware attack (2021)," NATO Cooperative Cyber Defence Center of Excellence, accessed October 2, 2025, https://cyberlaw.ccdcoe.org/wiki/Colonial_Pipeline_ransomware_attack_(2021).

[29] International Cyber Law: Interactive Toolkit, "Office of Personnel Management data breach (2025)," NATO Cooperative Cyber Defence Center of Excellence, accessed October 2, 2025, https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015); International Cyber Law: Interactive Toolkit, "SolarWinds (2020)," NATO Cooperative Cyber Defence Center of Excellence, accessed October 2, 2025, https://cyberlaw.ccdcoe.org/wiki/SolarWinds_(2020).

[30] Jenna McLaughlin, "Cyberattack on Red Cross compromised sensitive data on over 515,000 vulnerable people," NPR, January 20, 2022, https://www.npr.org/2022/01/20/1074405423/red-cross-cyberattack.

[31] Microsoft. "Microsoft Digital Defense Report: 600 Million Cyberattacks per Day around the Globe." CEE Multi-Country News Center, November 29, 2024. https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/.

[32] Google. "Threat Analysis Group." Google Blog. Accessed September 26, 2025. https://blog.google/threat-analysis-group/.

[33] Omer Yoachimik and Jorge Pacheco, "Record-Breaking 5.6 Tbps DDoS Attack and Global DDoS Trends for 2024 Q4," The Cloudflare Blog, January 21, 2025, https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/.

[34] European Repository on Cyber Incidents (EuRepoC), Cyber Incident Dashboard, accessed August 5, 2025, https://stats.eurepoc-dashboard.eu/.

[35] Nad'a Kovalčíková and Giuseppe Spatafora, The Future of Democracy: Lessons from the US Fight Against Foreign Electoral Interference, European Union Institute for Security Studies, Brief No. 22, December 2024, https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024.

[36] James Van de Velde, "When Does Election Interference via Cyberspace Violate Sovereignty? Violations of Sovereignty, 'Armed Attack,' Acts of War, and Activities 'Below the Threshold of Armed Conflict' via Cyberspace," in Jens David Ohlin, and Duncan B. Hollis (eds), Defending Democracies: Combating Foreign Election Interference in a Digital Age (New York, 2021; online edition, Oxford Academic, 17 June 2021), https://doi.org/10.1093/oso/9780197556979.003.0008, accessed 1 July 2025.

[37] Michael N. Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," Chicago Journal of International Law 19, no. 1 (Summer 2018), https://cjil.uchicago.edu/print-archive/virtual-disenfranchisement-cyber-election-meddling-grey-zones-international-law.

[38] Raphael Satter, "Microsoft Says It Caught Hackers from China, Russia, Iran Using Its AI Tools," Reuters, February 14, 2024, https://www.reuters.com/technology/cybersecurity/microsoft-says-it-caught-hackers-china-russia-iran-using-its-ai-

tools-2024-02-14/; Rob Garver, "Generative AI Makes Chinese, Iranian Hackers More Efficient, Report Says," Voice of America, January 29, 2025, https://www.voanews.com/a/generative-ai-makes-chinese-iranian-hackers-more-efficient-report-says/7956403.html.

39 Allison Pytlak and James Siebens, eds., Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches (Washington, D.C.: Stimson Center, July 2024), https://www.stimson.org/2024/advancing-accountability-in-cyberspace/.

40 Ibid., 6.

41 Michael J. Mazarr, Understanding Deterrence (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf; Quentin Hodgson, Logan Ma, Michael Fischerkeller, and Bryan Frederick, Modern Deterrence and Cyberspace: Translating Deterrence Theory to Practice (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

42 Pytlak and Siebens, eds., Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches.

43 UNODA, The UN Norms of Responsible State Behaviour in Cyberspace.

44 Christopher Ashley Ford, "Responding to Modern Cyber Threats with Diplomacy and Deterrence," U.S. Department of State, October 19, 2020, https://2017-2021.state.gov/responding-to-modern-cyber-threats-with-diplomacy-and-deterrence/.

45 A "red line" is a common term for explicitly stated conditions under which a party commits to using military force to prevent or reverse a particular course of action.

46 This same formula is sometimes expressed using different terms like "capability, determination, and declaration" in lieu of "credibility, resolve, and communication," but the basic concepts are the same; Cf., Inter-American Defense Board, Cyber Defense Handbook, January 2022, https://jid.org/wp-content/uploads/2022/01/Cyber-defense_handbook_ing.pdf.

47 Anne Neuberger, "China Is Winning the Cyberwar," Foreign Affairs, August 13, 2025, https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence.

48 UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, June 24, 2013.

49 Michael N. Schmitt, "Foreign Cyber Interference in Elections," International Law Studies 97, no. 1 (2021), https://digital-commons.usnwc.edu/ils/vol97/iss1/32/.

50 International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. United Nations, 2001. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

51 Michael N. Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," Chicago Journal of International Law 19, no. 1 (2018), https://cjil.uchicago.edu/print-archive/virtual-disenfranchisement-cyber-election-meddling-grey-zones-international-law. It should be noted that some states have questioned the applicability of due diligence obligations in cyberspace, presumably based on a desire to avoid the obligation.

52 Association of Southeast Asian Nations (ASEAN), Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace, February 2025, https://asean.org/wp-content/uploads/2025/02/ASEAN_checklist_print.pdf; 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.

53 Budapest Convention (ETS No. 185) and its Protocols," https://www.coe.int/en/web/cybercrime/the-budapest-convention, Council of Europe; United Nations, Convention on Cybercrime: Strengthening International Cooperation to Combat Crimes

Committed Through ICT Systems, adopted 24 December 2024, opened for signature 25–26 October 2025 in Hanoi, Viet Nam, and thereafter at UN Headquarters in New York until 31 December 2026, https://treaties.un.org/doc/Publication/CTC/Ch_XVIII_16.pdf.

54 Quentin E. Hodgson et al., Managing Response to Significant Cyber Incidents: Comparing Event Life Cycles and Incident Response Across Cyber and Non-Cyber Events (Santa Monica, CA: RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA198-1.html; James Siebens and Allison Pytlak, "Connecting 'Cyber Diplomacy' to 'Cyber Deterrence,'" Stimson Center, April 7, 2025, https://www.stimson.org/2025/connecting-cyber-diplomacy-to-cyber-deterrence/.

55 Cf., Tobias Feakin, "Calibrated Signals: How Middle Powers Are Rewriting the Rules of Cyber Attribution in the Indo-Pacific," The Diplomat, August 9, 2025, https://thediplomat.com/2025/08/calibrated-signals-how-middle-powers-are-rewriting-the-rules-of-cyber-attribution-in-the-indo-pacific/.

56 Kristen E. Eichensehr, "Cyberattack Attribution as Empowerment and Constraint," UCLA Law Review 67, no. 3 (2020): 618–676, https://www.uclalawreview.org/wp-content/uploads/securepdfs/2020/09/Eichensehr-67-3.pdf.

57 Andreas Kuehn, Debra Decker and Kathryn Rauhut, "Whodunit in Cyberspace: the Rocky Road from Attribution to Accountability," ORF America, December 11, 2023, https://orfamerica.org/newresearch/background-cyber-whodunit.

58 James Andrew Lewis, "Cyber Deterrence Declaratory Policy, 2011–2015," Strategic Technologies Blog, Center for Strategic and International Studies (CSIS), May 4, 2015, https://www.csis.org/blogs/strategic-technologies-blog/cyber-deterrence-declaratory-policy-2011-2015.

59 Royal United Services Institute, "Encouraging New Thinking on Offensive Cyber Operations," press release, September 15, 2025, https://www.wired-gov.net/wg/news.nsf/articles/encouraging+new+thinking+on+offensive+cyber+operations+15092025142500?open; Digital Watch Observatory, "UK to Establish Cyber and Electromagnetic Command to Enhance Warfare Capabilities," update, June 2, 2025, https://dig.watch/updates/uk-to-establish-cyber-and-electromagnetic-command-to-enhance-warfare-capabilities.

60 Center for Strategic and International Studies, "CSIS Launches Commission on Cyber Force Generation," press release, August 4, 2025, https://www.csis.org/news/csis-launches-commission-cyber-force-generation.

61 Eric Geller, "America's Cyber Ambassador on How to Spend $50 Million in Foreign Aid," The Record, April 22, 2024, https://therecord.media/cyber-foreign-aid-nathaniel-fick-state-department.

62 Department of National Defence (Canada), "Cyber Capabilities," Proactive Disclosure: Standing Committee on National Defence, April 24, 2023, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/secd-april-24-2023/cybercapabilities.html.

63 François Delerue, Alix Desforges, and Aude Géry, "A Close Look at France's New Military Cyber Strategy," War on the Rocks, April 23, 2019, https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/; International Institute for Strategic Studies, Cyber Capabilities and National Power: France, IISS Research Paper, June 2021, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---france.pdf.

64 International Institute for Strategic Studies, Cyber Capabilities and National Power: France, June 2021, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---france.pdf.

65 Paul Rosenzweig, "Volt Typhoon and the Disruption of the U.S. Cyber Strategy," Lawfare, March 5, 2024, https://www.lawfaremedia.org/article/volt-typhoon-and-the-disruption-of-the-u.s.-cyber-strategy.

66 Allison Peters and Pierce MacConaghy, "Unpacking US Cyber Sanctions," Third Way, February 10, 2021, https://www.thirdway.org/memo/unpacking-us-cyber-sanctions.

67 Louise Marie Hurel, "The Challenge of Non-Western Cyber Attribution," Royal United Services Institute (RUSI), video commentary, May 29, 2025, https://www.rusi.org/news-and-comment/video-commentary/challenge-non-western-cyber-attribution.

[68] International Law Commission, Responsibility for States for Internationally Wrongful Acts, United Nations, 2001, Arts, 22 and 49, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

[69] Talita Dias, Countermeasures in International Law and Their Role in Cyberspace, Chatham House, May 23, 2024, https://www.chathamhouse.org/2024/05/countermeasures-international-law-and-their-role-cyberspace.

[70] Counter Ransomware Initiative, "About Us," accessed October 2, 2025, https://counter-ransomware.org/aboutus.

[71] James Andrew Lewis, "Next Steps for the International Counter Ransomware Initiative," Center for Strategic & International Studies, January 21, 2025, https://www.csis.org/analysis/next-steps-international-counter-ransomware-initiative.

[72] Louise Marie Hurel and Gareth Mott, Rethinking Cyber Deterrence in a Multipolar World (London: Royal United Services Institute, August 2025), 9, https://static.rusi.org/rethinking-cyber-deterrence-in-a-multipolar-world.pdf. See also Jon R. Lindsay and Erik Gartzke, eds., Cross-Domain Deterrence: Strategy in an Era of Complexity (Oxford: Oxford University Press, 2019).

[73] Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace" (PhD diss., Columbia University, 2017), in Cyber Power and the International System, accessed August 5, 2025, https://core.ac.uk/download/161457334.pdf.

[74] Amos C. Fox, "Conflict and the Need for a Theory of Proxy Warfare," Journal of Strategic Security 12, no. 1 (2019): 44–71, https://digitalcommons.usf.edu/jss/vol12/iss1/3/.

[75] Hurel and Mott, Rethinking Cyber Deterrence in a Multipolar World, 10.

[76] Kelly McCoy, "In the Beginning, There Was Competition: The Old Idea Behind the New American Way of War," Modern War Institute, April 11, 2018, https://mwi.westpoint.edu/beginning-competition-old-idea-behind-new-american-way-war/.

[77] Yoram Dinstein, "Computer Network Attacks and Self-Defense," in Computer Network Attack and International Law, ed. Michael N. Schmitt and Brian T. O'Donnell, vol. 76 of US Naval War College International Law Studies, 99-114 (Newport, RI: Naval War College, 2002), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1075&context=ils.

[78] E.g., Yuval Shany and Michael N. Schmitt, "An International Attribution Mechanism for Hostile Cyber Operations," International Law Studies 96, no. 1 (2020): 155–178, https://digital-commons.usnwc.edu/ils/vol96/iss1/8/.

[79] European Union Agency for Cybersecurity (ENISA), CSIRTs Network, accessed August 6, 2025, https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network.

[80] Foreign, Commonwealth & Development Office (UK), The Pall Mall Process: Code of Practice for States, GOV.UK, April 4, 2025, https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states.

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

STIMSON.ORG

STIMSON

INNOVATIVE IDEAS CHANGING THE WORLD