INTERNATIONAL LAW STUDIES

Published Since 1895

Enhancing Accountability in Cyberspace Through a Three-Tiered International Governance Regime

Dan Efrony

103 INT'L L. STUD. 396 (2024)

Volume 103

2024

Published by the Stockton Center for International Law

ISSN 2375-2831

Enhancing Accountability in Cyberspace Through a Three-Tiered International Governance Regime

Dan Efrony[*]

CONTENTS

* PhD Candidate, Faculty of Law, Hebrew University of Jerusalem. Formerly, Chief Military Advocate of the Israel Defense Forces. The author is particularly indebted to Yuval Shany for his guidance and insightful comments on the draft of this article.

The thoughts and opinions expressed are those of the author and not necessarily those of the State of Israel, the Israel Defense Forces, the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

> "No nation is more committed than the United States to combating the biological [cyber] weapon threat. . . . It will require new and innovative paradigms to deal with the magnitude of biological [cyber] activity that can be a threat, the explosively changing technology in the biological [cyber] fields, and the varied potential objectives of a biological [cyber] weapons program. We simply cannot try to patch or modify the models we have used elsewhere."[1]

Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Unlike the physical nature of all other domains, cyberspace is virtual and, consequently, omnipresent, overlapping with all other domains. In fact, its evolving technologies have become indispensable for the greater part of communication and activity, and have an immediate tangible impact, for better or worse, on reality in any domain. This creates incredible opportunities as well as formidable risks. The latter are reflected by thousands of daily, clandestine, highly sophisticated, criminally and politically motivated cyber operations.[3] Neutralizing these risks requires a high degree of cooperation among the community of States, especially among the leading cyber power States.[4] This has become, however, an exceedingly difficult challenge to meet and is currently out of reach.

---

1. Statement by Ambassador Donald Mahley, U.S. Special Negotiator for Chemical and Biological Arms Control Issues, to the Ad Hoc Group of Biological Weapons Convention Parties (July 25, 2001), https://2001-2009.state.gov/t/ac/rls/rm/2001/5497.htm (replacing "biological" with "cyber" makes this quotation a perfect fit to describe the great challenges of the present cyber era).

2. *Cyberspace*, UNITED STATES GOVERNMENT COMPENDIUM OF INTERAGENCY AND ASSOCIATED TERMS 233 (Nov. 2019), https://www.jcs.mil/Portals/36/Documents/Doctrine/dictionary/repository/usg_compendium.pdf.

3. In this article "cyber attacks," "cyber operations," and "cyber activities," are used interchangeably. However, the article focuses on politically motivated incidents; that is, cyber attacks conducted by States through their official organs and agents or through third parties as proxies.

4. *See* JULIA VOO ET AL., NATIONAL CYBER POWER INDEX 2020: METHODOLOGY AND ANALYTICAL CONSIDERATION (Sept. 2020), https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (This research study produced a model for assessing

The great powers—China, Russia, and the United States—have been intensively engaged in a Great Power Competition in which China and Russia challenge elements of the Western-led international order.[5] Both challenge-posing States "want to shape a world antithetical to U.S. values and interests."[6] They seek to reinforce their deterrent capabilities and increase their impact on the international order. This is at the expense of American hegemony and power supremacy, which the United States is determined to preserve to ensure its deterrence supremacy.[7] The recent Russian invasion of Ukraine is a troubling illustration of this competition, pushing the world into a serious global crisis, perhaps even to the brink of a nuclear conflict.[8] The invasion led the Russian regime to maximize the level of risks and costs it was willing to bear to ensure its centrality as a leading superpower. Such a motivation cannot be underestimated when considering the Great Power Competition's impact on emerging technological capabilities, the cyber arms race, and cyber conflicts. Additionally, it poses a challenge in shaping State practice and international law in cyberspace and has direct repercussions on all other dimensions, including outer space.[9] Consequently, the world has

---

the cyber power of States based on open-source intelligence and relevant criteria. The researchers identified thirty States that retain proven cyber power [hereinafter cyber power States]. Obviously, the number always increases. The top ten include the UN Security Council's five permanent members.).

5. ANTHEA ROBERTS, IS INTERNATIONAL LAW INTERNATIONAL? 286 (2017); *see also* RONALD O'ROURKE, CONG. RSCH. SERV., R43838, RENEWED GREAT POWER COMPETITION: IMPLICATIONS FOR DEFENSE—ISSUES FOR CONGRESS (Mar. 10, 2022). For further reading on this phenomenon, *see* Jonathan M. DiCicco & Tudor A. Onea, *Great-Power Competition*, OXFORD RESEARCH ENCYCLOPEDIA: INTERNATIONAL STUDIES (Jan. 31, 2023), https://doi.org/10.1093/acrefore/9780190846626.013.756.

6. THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 25 (Dec. 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

7. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 4 (Feb. 7, 2022), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf (pointing to "the growing specter of great power competition and conflict . . . . China increasingly is a near-peer competitor, challenging the United States in multiple arenas . . . and is pushing to change global norms . . . . Russia is pushing back against Washington where it can—locally and globally . . . ."); *see also* THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 8–9, 23–27 (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

8. *See* O'ROURKE, *supra* note 5.

9. DEFENSE INTELLIGENCE AGENCY, 2022 CHALLENGES TO SECURITY IN SPACE (Apr. 12, 2022), https://www.dia.mil/Portals/110/Documents/News/Military_Power_

become a digital, global battle zone driven by the Great Power Competition and conflicting geopolitical interests.[10]

Moreover, this competition has emerged as a significant impediment to international efforts aimed at achieving a consensus for transforming the international legal framework into a universal, clear, updated, and binding scheme in cyberspace. During 2000–2021, the most significant channel for those efforts was the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter the UN-GGE). This group narrowly succeeded in reaching consensus during its third and fourth rounds of discussions in 2013 and 2015, respectively. It affirmed the principle that international law, particularly the UN Charter, is applicable to cyberspace and agreed on a list of eleven non-binding norms for responsible State behavior in cyberspace (the "List of Non-Binding Norms").[11] The fifth round of the UN-GGE (2016–17) failed to extend the scope of the consensus and collapsed. Nevertheless, the UN General Assembly (UNGA) approved two resolutions initiating two parallel tracks—the Open-Ended Working Group and the Sixth UN-GGE—with largely overlapping mandates.[12] The endorsement of these parallel tracks exemplifies the two intertwined, yet at times contradictory, trajectories that characterize the Great Power Competition.

Publications/Challenges_Security_Space_2022.pdf (arguing that the combined in-orbit space fleets of China and Russia grew more than 70 percent in just over two years, indicating both nations' intent to undercut U.S. and allied global leadership in the space domain).

10. *See The United States Announces Export Controls to Restrict China's Ability to Purchase and Manufacture High-End Chips*, 117 AMERICAN JOURNAL OF INTERNATIONAL LAW 144 (2023).

11. Secretary-General Transmittal of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶¶ 13, 28, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter List of Non-Binding Norms] (paragraph 13 includes the List of Non-Binding Norms and paragraph 28 offers "non-exhaustive views" on principles of international law, such as sovereign equality, due diligence, and the prohibitions on use of force and non-intervention, that should apply to cyberspace).

12. *See* G.A. Res. 73/27, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Dec. 5, 2018) (approving Russia's proposal to establish an Open-Ended Working Group instead of the UN GGE and allowing all UN member States to participate as full members of the group and permitting relevant regional organization and NGOs to share their views); G.A. Res. 73/266, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Dec. 22, 2018) (approving the U.S. proposal, resuming the UN-GGE channel by establishing the sixth UN GGE in parallel track, and allowing any interested State or regional organization to share its views with the governmental experts, unlike the previous UN GGEs).

Given that the UN-GGE and the Open-Ended Working Group operated on a consensus basis, competing sides had the ability to impede or neutralize each other's efforts in pursuing their respective political goals. Finally, both groups reached mutual consensus and concluded their work with unanimous final reports.[13] However, they failed to record any significant breakthrough toward resolving major political and legal obstacles to the application of international law to cyberspace.[14]

Nevertheless, December 2021 marked progress when a new UNGA resolution approved a joint U.S.-Russian proposal to merge both tracks into one, under the Open-Ended Working Group.[15] This important development was the result of bilateral negotiations, suggesting, in turn, that despite the Great Power Competition, bilateral strategic cooperation between Russia and the United States, though difficult, was still attainable. However, the Russian invasion of Ukraine appears to have reshuffled the cards in this regard. As a result, bilateral strategic cooperation and negotiations halted at once.[16]

This backdrop underlines two interrelated premises regarding the global interest in adjusting international law to cyberspace. First, the Great Power Competition has become a restricting factor, of an increasingly intense and significant scope and severity, as described above. Consequently, resolving the conflicting political interests associated with the Great Power Competition, or minimizing their adverse ramifications through the establishment of

---

13. *See* Secretary-General Transmittal of the Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N. Doc. A/76/135 (July 14, 2021); Secretary-General Transmittal of the Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/75/816 (Mar. 18, 2021).

14. Dan Efrony, *The UN Cyber Groups, GGE and OEWG—A Consensus is Optimal, But Time is of the Essence*, JUST SECURITY (July 16, 2021), https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensUS-is-optimal-but-time-is-of-the-essence/ (criticizing the consensus requirement and its mutual neutralizing impact on both tracks).

15. G.A. Res. 76/19 (Dec. 8, 2021). For more details about the U.S.-Russia negotiations that led to this resolution, *see* Elena Chernenko, *Binary Code, Russia and the United States Submitted a Joint Resolution on Cybersecurity to the UN*, KOMMERSANT (Oct. 17, 2021), https://www.kommersant.ru/doc/5038983 (translated from Russian by Google Translate).

16. *See* Carly Page, *Russia's FSB "Shuts Down" Notorious REvil Ransomware Gang*, TECHCRUNCH (Jan. 14, 2022), https://techcrunch.com/2022/01/14/fsb-revil-ransomware/; TASS, *US Unilaterally Shuts Down Communication Channel with Russia on Cybersecurity—Official* (Apr. 7, 2022), https://tass.com/world/1434321.

States' accountability relying on distinct State practice or a universal binding convention, seem unattainable.[17] Yet this is not an all-or-nothing situation. Detecting cyber attacks and attributing responsibility are key elements in holding States or entities accountable for their wrongdoing in cyberspace, even in the absence of a formal convention. However, it is important to note that accountability encompasses a broader scope of objectives than legal responsibility. While the latter is confined to legal relations, obligations, and consequences arising from international law, accountability extends further. It includes responsibility towards individual persons regardless of applicable laws, encompasses political aspects, such as the duty to account for the exercise of power, and incorporates norms of good governance and transparency.[18]

The second premise is that the approach implemented by the Great Powers, especially the United States, has been one of constructive and flexible legal ambiguity, including with respect to reaching consensus on the text of the final reports of the UN groups (the UN-GGE and the Open-Ended Working Group). This ambiguity preserves accountability gaps that provide these powers with flexibility to maintain a qualitative edge over their rivals. It also allows them to portray themselves as abiding by rules of customary international law, though the precise content of these laws in cyberspace remains ambiguous.[19] While a growing number of States have partially clarified

17. *See* Chernenko, *supra* note 15; *see also* Kenneth Corbin, *State Department Argues Against "Cyber Arms" Treaty*, CIO (May 26, 2016), https://www.cio.com/article/238152/state-department-argues-against-cyber-arms-treaty.html.

18. JAMES CRAWFORD, THE FRAMEWORK OF RESPONSIBILITY 84–85 (2013).

19. Michael Byers, *Still Agreeing to Disagree, International Security and Constructive Ambiguity*, 8 JOURNAL ON THE USE OF FORCE AND INTERNATIONAL LAW 91 (2021) (defining "constructive ambiguity" as the deliberate use of ambiguous language to achieve agreement during the negotiation of a legal text. *Id.* at 93.); *see also* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AMERICAN JOURNAL OF INTERNATIONAL LAW 583, 696 (2018) (most States active in cyberspace implement flexible ambiguity about their legal and political approaches to preserve a technical qualitative advantage and maneuverability to protect their national interests); Sean Watts, *Cyber Law Development and the United States Law of War Manual*, *in* INTERNATIONAL CYBER NORMS LEGAL, POLICY & INDUSTRY PERSPECTIVES 49, 63 (Anna-Maria Osula & Henry Rõigas eds., 2016), https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch3.pdf (claiming that the *U.S. Law of War Manual* includes persistent ambiguities in the operation of the law of war in cyberspace. Leaving those ambiguities unresolved is "strong evidence of the U.S. comfort with these uncertainties and legal voids," suggesting an American inclination "against definitive clarity and precision in this challenging domain of state competition.").

their views regarding disputed legal issues related to these rules or norms, achieving normative clarity and transparency in cyberspace remains a distant goal. This affects the List of Non-Binding Norms's compliance pull vis-à-vis States and narrows the odds of legally attributing State responsibility for violating any norm of the List whose content and outer boundaries are still contested. As a corollary of both premises, the Great Powers do not exert sufficient efforts to reach a consensus on a balanced approach that they can accept, respect, and implement to foster global cooperation in countering cyber threats. On the contrary, each power sticks to its own competing strategy and acts accordingly. Russia and China have undertaken significant steps within their political networks to avert the free flow of information. Both consider it a serious threat to their respective regime's stability and homeland security.[20] The United States, on its part, is dedicated to preserving its deterrent supremacy and the American-led liberal international order.[21]

In light of the above, it is no surprise that extensive inter-State cyber attacks have failed to spark the establishment of a binding international convention and an acceptable international law enforcement mechanism. Instruments and mechanisms of this nature are essential to significantly reduce the risks associated with advanced cyber capabilities and restrain States' temptation to exploit these capabilities and engage in illicit, covert cyber operations. However, achieving consensus among the Great Powers on establishing the elements of a functioning international legal cybersecurity regime currently seems like a pipe dream. The upshot is a vicious cycle. This article addresses this cycle and proposes workable solutions.

The article proceeds as follows: Part II depicts the embryonic stage of the international normative layer in cyberspace, which has been confined thus far to UNGA resolutions that underpin the List of Non-Binding Norms

20. Matt Burgess, *Russia Is Quietly Ramping Up Its Internet Censorship Machine*, WIRED (July 25, 2022), https://www.wired.com/story/russia-internet-censorship-splinternet/ (The Russian sovereign law empowers the government to block websites, helping to build upon the idea of the RuNet, a Russian internet that can be disconnected from the rest of the world); *see also* Elizabeth C. Economy, *The Great Firewall of China: Xi Jinping's Internet Shutdown*, THE GUARDIAN (June 29, 2018), https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown; Valentin Weber, *The Worldwide Web of Chinese and Russian Information Controls*, UNIVERSITY OF OXFORD, CENTRE FOR TECHNOLOGY AND GLOBAL AFFAIRS (Working Paper Ser. No. 11, Sept. 2019), https://www.politics.ox.ac.uk/sites/default/files/2022-03/201909-CTGA-Weber-V-webofchineseandrussianinfo.pdf (describing information control techniques and analyzing their global diffusion, particularly to affiliated authoritarian regimes).

21. *See* NATIONAL SECURITY STRATEGY, *supra* note 7.

as reflecting responsible State behavior. The article elaborates on this normative layer's major weaknesses and their repercussions for the List's effectiveness and State compliance. A discussion of the critical issue of legitimacy addresses how it affects the List of Non-Binding Norms's effectiveness and how legitimacy could be a "force multiplier" in augmenting the normative layer and international governance in cyberspace. Section B of Part II explores several attempts to establish international instruments to legitimately reinforce compliance and deterrence. The results have so far been poor, generating a vicious cycle, but not reaching a dead end. Part III challenges U.S. policy and proposes a modular, three-tiered program ("Triple I"), which relies on the premise that universal consensus—or interchangeably, consensus of the five permanent members of the Security Council (P5)—is out of reach in the near future due to the Great Power Competition. Thus, a "workable consensus" is an essential enabler for incrementally establishing a global framework of a governance regime—a "Triple I." At the first stage, the establishment of an independent International Cyber Attribution Mechanism, serving as a keystone for maintaining State accountability and as an important confidence-building measure towards formulating, possibly even concurrently, the International Cyber Security Initiative. The Cyber Security Initiative would serve as an international cyber security arm to bolster deterrence through collaboration in defense and resilience. Finally, and no less importantly, an International Cyber Law Convention, though more challenging, is crucial for underpinning the international legal framework in cyberspace with a clear and widely accepted normative layer. Part IV concludes.

II. WEAKENED NORMATIVE LAYER

International cyber law is still in its embryonic stages. Thus far, it relies on UNGA resolutions, including the List of Non-Binding Norms, for responsible State behavior in cyberspace. At most, these resolutions are recommendations or declarative international instruments that can be considered "soft law."[22] As such, they may contribute to the future development of State practice, which over the years may transform into customary international law.

22. *See generally* Oscar Schachter, *The Twilight Existence of Nonbinding International Agreements*, 71 AMERICAN JOURNAL OF INTERNATIONAL LAW 296, 303 (1977) (These are political or moral commitments, and noncompliance with them cannot be grounds for sanctions or claims for reparation or judicial remedies.); *see also* A. T. Guzman & T. L. Meyer, *International Soft Law*, 2 JOURNAL OF LEGAL ANALYSIS 172, 216–21 (2010) (arguing that General Assembly resolutions are widely acknowledged to impact the legal obligations of States); Rüdiger

Naturally, fostering cooperation and compliance with binding rules by utilizing coercive measures is more complicated and less practical in the international arena than in the domestic arena.[23] This challenge becomes far more complex in cyberspace when cooperation and compliance are sought in connection with non-binding norms of responsible State behavior. This is indeed the case, against the backdrop of an intensifying Great Power Competition, a contested attribution process, and lack of consensus on how to interpret and apply these non-binding norms to cyberspace. As the next paragraphs shall demonstrate, this normative layer is less effective in compelling States to align their behavior with those norms.[24] Ultimately, this outcome adversely affects the international community's ability to deter by attributing responsibility and holding States accountable for their cyber wrongdoings.

A. Repercussions on Effectiveness and Compliance

States accede to international instruments only by consent, exercising their own free political will. Unsurprisingly, they often decline to accede to binding treaties that recognize the compulsory jurisdiction of independent and impartial law enforcement mechanisms. The international community tends to compensate such reluctance to commit by embracing a pragmatic approach.[25] Accordingly, compliance systems established by international instruments might concentrate on verification by cooperation and coordination instead of mandatory law-enforcement or punitive measures. These latter measures are confined to the exclusive authority of the UN Security Council, mostly under the relevant international treaty.[26] Furthermore, having the P5 on board might significantly increase the likelihood of persuading

---

Wolfrum & Jakob Pichon, *Consensus*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, ¶¶ 23–24, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1387?rskey=4NQHNO&result=15&prd=OPIL.

23. Jack L. Goldsmith & Eric A. Posner, *The Limits of International Law Fifteen Years Later*, 22 CHICAGO JOURNAL OF INTERNATIONAL LAW 110, 114 (2021) (claiming that due to the lack of any neutral, reliable, and centralized enforcer of international law, States must account for incentives to make and comply with international law).

24. Timothy Meyer, *How Compliance Understates Effectiveness*, 108 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 93 (2014) (distinguishing effectiveness from compliance: compliance refers to whether a State's conduct meets the prescribed legal standard, while effectiveness refers to whether the law's enactment changed the State's behavior).

25. Wyn Q. Bowen et. al., *Multilateral Cooperation and the Prevention of Nuclear Terrorism: Pragmatism over Idealism*, 88 INTERNATIONAL AFFAIRS 349, 362 (2012).

26. Reviewing international treaties in the realm of weapons of mass destruction leads to the conclusion that the treaties' organs are authorized—by a qualified majority that could

allies to accede to the treaty in question and embrace its verification system. After all, they would remain assured that, in a worst-case scenario, they would be politically protected by their ally through its veto power.

Under such conditions, State compliance can usually be expected with respect to binding or non-binding international provisions that implement the pragmatic approach. Nonetheless, States may still minimize or evade compliance with specific international provisions, especially if they can get away with undetected violations.[27] In doing so, States prioritize more important national interests at the expense of other national and international interests, such as harming the State's reputation as a law-abiding State or exposure to the risks of formal or informal sanctions.[28]

Nevertheless, even if the establishment of binding international law faces legal and political obstacles, States concerned about their reputation as law-abiding entities might nonetheless be mindful of their international reputation as responsible actors. Consequently, they might expend efforts to avert accountability even in the court of public opinion—a legitimacy court—for

---

easily be affected by the geopolitical division—to undertake limited administrative measures against a State that declines cooperation. More serious and punitive measures such as imposing international sanctions fall under the authority of the UN Security Council and its veto regime. *See, e.g.*, RALF TRAPP, COMPLIANCE MANAGEMENT UNDER THE CHEMICAL WEAPONS CONVENTION 18–19 (WMD Compliance & Enforcement Series, Paper 3, 2019), https://www.unidir.org/sites/default/files/2019-12/UNID%20WMD%20CE%20-%20Paper%203%20v3.pdf.

27. JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 13 (2005) (asserting "international law does not pull states toward compliance contrary to their interest"). Scholars have criticized this approach, which they perceived as negating the role of international law. See their response to this criticism, Goldsmith & Posner, *supra* note 23, at 119 (reiterating that international law has a robust role in fostering international coordination and cooperation. Still, complying with international law in each situation is considered with other important national interests.).

28. ABRAM CHAYES & ANTONIA H. CHAYES, THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS 152, 230 (1998) (arguing that reputation effects induce treaty compliance. The threat of exposure and shaming, not material sanctions, is "a powerful spur for action" since "a reputation for reliability matters."). For a more reserved approach, *see* George W. Downs & Michael A. Jones, *Reputation, Compliance, and International Law*, 31 JOURNAL OF LEGAL STUDIES 95, 113 (2002) (claiming "reputation matters, just not so much as some might like"); Andrew T. Guzman, *Reputation and International Law*, 34 GEORGIA JOURNAL OF INTERNATIONAL & COMPARATIVE LAW 379 (2006).

illegitimate activities conducted against the interests of other States or the global community.[29]

Still, State compliance with the List of Non-Binding Norms remains limited, as reflected by the frequent recurrence of State-sponsored cyber attacks in violation thereof. This raises a dilemma: should the international community strive to increase the degree of compliance with the List by replacing it with a new, binding international treaty, which might also include measures to verify compliance, or alternatively focus on finetuning the legal interpretation of existing List norms, to clarify them and simplify their implementation, thereby increasing compliance?

A review of recent developments in the field shows that the international community sits on both sides of the fence with an extremely limited degree of success due to the conflicting strategic interests of the Great Powers. Recent final reports by the Open-Ended Working Group and the UN-GGE-2021 reiterated basic consensus on the List of Non-Binding Norms.[30] However, neither have clarified if and how important international norms and principles such as sovereignty, due diligence, non-intervention, espionage, and the use of force apply to cyberspace. More disturbingly, they have not addressed the need for attribution through a credible mechanism or agreed primary and secondary rules to eliminate or drastically reduce the "plausible deniability" shield. Thus far, this has allowed States to violate nonbinding norms while simultaneously denying claims of State responsibility.

Nevertheless, Russia has officially reiterated its preference for replacing the voluntary List of Non-Binding Norms with a legally binding UN convention regulating State relations on the security and use of information and communications technologies.[31] Despite this lip service, in practice both

29. Risse Thomas & Kathryn Sikkink, *The Socialization of International Human Rights Norms into Domestic Practices*, *Introduction*, *in* THE POWER OF HUMAN RIGHTS: INTERNATIONAL NORMS AND DOMESTIC CHANGE 1, 38 (Thomas Risse et al. eds., 1999).

30. *See* U.N. Doc. A/76/135, *supra* note 13; Efrony, *supra* note 14.

31. Press Release, Ministry of Foreign Affairs of the Russian Federation, The Concept of the UN Convention on International Information Security (May 16, 2023), https://www.mid.ru/en/foreign_policy/news/1870609/ (unofficial translation available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf) (unsurprisingly including the main principles of the Shanghai Cooperation Organization International Code of Conduct for Information Security included in Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Secretary General, U.N. Doc. A/69/723 (Jan. 13, 2015)).

Russia and China have failed to demonstrate a genuine willingness—as witnessed in the last four rounds of the UN-GGE (2013, 2015, 2017, and 2021) and during the enduring discussions of the Open-Ended Working Group—to make significant strides toward a new convention, unless its provisions align with their authoritarian ideology and national strategic interests.

Unsurprisingly, the United States and its close allies consistently and firmly reject this approach. Thus, the principal American approach opposes the idea of establishing a new binding treaty.[32] During the Open-Ended Working Group discussions in 2021 and subsequent Russian-American discourse, Michele Markoff, the head of the U.S. delegation, depicted the idea of establishing a new global convention as "impractical" for three reasons.[33] First, there are States that still refuse to explicitly confirm that the basic elements of existing international law apply to cyberspace and are unwilling to comply with the List of Non-Binding Norms. Second, creating a legally binding global convention would take years and could already be outdated by the time of its arrival due to rapidly emerging technology. Third, information and communications technologies are not susceptible to traditional arms control arrangements. However, the following statement by Thomas Franck, published seventeen years ago, could shed light on the more authentic and convincing motives underpinning the U.S. stance in general, let alone amid the Great Power Competition:

---

32. For arguments regarding the unlikelihood of establishing an international cybersecurity treaty, *see* Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL LAW REVIEW 565, 640–42 (2018) (explaining why it is unlikely to foresee a comprehensive cybersecurity treaty and citing helpful references); *see also* Jack Goldsmith, *Cybersecurity Treaties—A Skeptical View* (Hoover Institution, Future Challenges Essay, 2011), https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf; Michael N. Schmitt & Liis Vihul, *The Emergence of International Legal Norms for Cyberconflict*, *in* BINARY BULLETS: THE ETHICS OF CYBERWARFARE 34, 44 (Fritz Allhoff, Adam Henschke & Bradley J. Strawser eds., 2016) (for a responsive view, *see* Mette Eilstrup-Sangiovanni, *Why the World Needs an International Cyberwar Convention*, 31 PHILOSOPHY & TECHNOLOGY 379 (2018)).

33. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Compendium of Statements in Explanation of Position on the Final Report, U.N. Doc. A/AC.290/2021/INF/2, at 85–86 (Mar. 25, 2021), https://front.un-arm.org/wp-content/uploads/2021/04/A-AC.290-2021-INF-2.pdf (text of the U.S. explanation of its position); *see also* Chernenko, *supra* note 15 (translated to English by Google Translate) (pointing to the voluntary nature of the List of Non-Binding Norms as a weakness and recalling that Russia has previously repeatedly proposed to make those norms legally binding while the United States has always opposed it).

> [W]hen a nation is the world's only superpower, why should it permit itself to be bound by norms and rules that may not always produce results that accrue to its advantage? Why should any state, in deference to law, ever forgo a realizable advantage and accept an outcome that does not maximize its national interest?[34]

The U.S. preference for the List of Non-Binding Norms as a soft law measure over a new binding universal treaty may conform with what scholars have already identified as "a decline in the use of binding international instruments and a rise in the use of 'non–binding' political commitments to foster international cooperation."[35] This is accompanied by the risk of being subject only to a political or moral response in case of non-compliance.[36]

Kal Raustiala points to the following advantages of embracing this line of action.[37] First, it is easier and faster to agree on a non-binding treaty and to give it effect. Second, States that care about compliance tend to embrace standards that are not too demanding, and favor them over more binding, stringent ones that might raise uncertainties about the feasibility of full compliance.[38] Third, State experience in some international realms, like the monetary, trade, and environmental fields, suggests that non-binding commitments provide States with greater flexibility and willingness to consider ambitious or experimental approaches to international cooperation. States, in fact, have in many cases succeeded in complying with such non-binding commitments even though they were more ambitious than binding ones.[39] Finally, commitments, even non-binding commitments, become more effec-

34. Thomas M. Franck, *The Power of Legitimacy and the Legitimacy of Power: International Law in an Age of Power Disequilibrium*, 100 AMERICAN JOURNAL OF INTERNATIONAL LAW 88, 89 (2006).

35. *See* Posner & Goldsmith, *supra* note 23, at 126.

36. *See* Schachter, *supra* note 22.

37. Kal Raustiala, *Compliance & Effectiveness in International Regulatory Cooperation*, 32 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 387, 423–27 (2000) (explaining the advantages of non-binding international instruments relying on examples from the international environmental, monetary, and trade fields).

38. *Id.* at 397, 425.

39. *Id.* at 425; *see also* Kal Raustiala & David G. Victor, *Conclusion*, *in* THE IMPLEMENTATION AND EFFECTIVENESS OF INTERNATIONAL ENVIRONMENTAL COMMITMENTS: THEORY AND PRACTICE 659, 685 (David G. Victor, Kal Raustiala & Eugene B. Skolnikoff eds., 1998).

tive when they are linked to well-developed and regularized systems of implementation review.[40] Thus, non-binding treaties may be sometimes as effective, and at times even more effective, than legally binding treaties. Effectiveness is measured by the extent to which legal norms induce changes in State behavior.[41] Usually, States accede to an international treaty only if they fully understand their obligations under that treaty. Considering the extent to which those norms, whether binding or non-binding, truly reflect its preexisting preferred "State behavior," they could, consequently, generate full compliance. When this is the case, the degree of compliance with the treaty's provisions is usually high, while the effectiveness—in the sense of changing State behavior—is low.[42]

Despite the advantages of non-binding treaties, the United States has chosen not to formalize the List of Non-Binding Norms, and the consensus reached thus far, into such a treaty. Furthermore, in an underregulated, evolving domain like cyberspace, even non-binding international treaty provisions would require the parties to remove, or at the very least reduce, legal ambiguities. This could be achieved, for instance, by redefining the legal boundaries of "sovereignty," "due diligence," and legitimate versus prohibited "espionage." Additionally, in the given circumstances of an intensifying Great Power Competition, emerging technological capabilities, and the prominent U.S. strategic interest in preserving its technological deterrent supremacy, any normative clarification made by law-abiding States like the United States and the United Kingdom, and embraced by other like-minded States, may primarily restrain them, and to a far lesser extent, if at all, the authoritarian regimes operating in the field.[43]

As a corollary, in the absence of normative clarity, the United States and its close allies do not purport to assign legal responsibility to foreign States for conducting harmful cyber attacks. Rather than specifying which international rule the aggressor State has breached, they hold it accountable for acting contrary to an opaque standard—"responsible State behavior"—and determine whether to retaliate through retorsions. These are unfriendly acts,

40. Raustiala, *supra* note 37, at 425.

41. *Id.* at 394; *see also* Meyer, *supra* note 24.

42. Raustiala, *supra* note 37, at 394 (when the legal standard imitates or falls below the baseline, compliance with such standards is high but the effectiveness—the desired change in State behavior—is low).

43. Roberts, *supra* note 5, at 313 (summarizing the conflicting approaches of the United States—United Kingdom on one hand and China-Russia on the other—regarding the establishment of a universal treaty).

but lawful under international law and are found within the prerogatives of every State. Thus, resorting to them does not need to be justified by reference to a defined preceding violation.

The List of Non-Binding Norms's non-binding language, and its inherent ambiguity regarding international legal terms and principles in the context of international cyber operations, preclude coercive options for ensuring compliance.[44] Moreover, it allows the United States and its close allies to exercise flexible discretion in distinguishing between violations likely to lead to legal attribution of State responsibility for violating defined international rules or obligations along with some form of response, and those unlikely to lead to such attributions whether or not accompanied by a response ("gradations in law enforcement").[45] Ultimately, the List of Non-Binding Norms's ability to pull States to change their behavior in cyberspace and comply with voluntary norms remains limited; however, it correlates with legitimacy. Prominent levels of effectiveness in applying voluntary norms and ensuring State compliance indicate parallel degrees of legitimacy and vice versa.[46]

The following section delves into the legitimacy factor, exploring its theoretical foundations and practical manifestations. To what extent has it been realized in the formation and implementation of the normative layer? What conditions are necessary for legitimacy to function as a force multiplier, enhancing the normative layer and legitimizing processes and their outcomes?[47] Insights gained from this discussion could be embraced and implemented in shaping the emerging international governance of cyberspace.

---

44. A discussion of other factors in ensuring compliance, such as coercion and self-interest, is beyond the scope of this article.

45. Efrony & Shany, *supra* note 19 at 650–52.

46. Hugo Siblesz, *The Role of International Organizations in Fostering Legitimacy in Dispute Resolution*, *in* INTERNATIONAL ORGANIZATIONS AND THE PROMOTION OF EFFECTIVE DISPUTE RESOLUTION 77, 80 (Peter Quayle & Xuan Gao eds., 2019) (arguing that legitimacy increases effectiveness by increasing compliance and assisting in developing further legitimization of the set of norms that constitute the regime).

47. Addressing the extensive literature on the concept of legitimacy and its various perspectives in a wide range of disciplines is beyond the scope of this article. Thus, the discussion of legitimacy in the following Parts of this article shall be limited to the context of the challenge of shaping and effectively applying international law to cyberspace and establishing relevant international governance institutions.

B. Legitimacy as a Force Multiplier

The most significant factor that is necessary, yet insufficient, for meeting the challenge of compliance with international regulation and, specifically, with non-binding norms, is legitimacy. This is because "the language of legitimacy and the language of crisis have long been associated with each other, standing, as they both do, at the borders of order and chaos."[48] Legitimacy, strong or weak, may tip the scale between these two trajectories, primarily on the transnational level, in which law enforcement merely relies on incentives and sanctions, or on State compliance resulting from the norm's perceived legitimacy.[49]

In his seminal study on legitimacy, Thomas Franck points to the nexus between legitimacy and voluntary compliance. He defines the former as "a property of a rule or rule-making institution which itself exerts a pull towards compliance" on nations, international organizations, leadership elites, and, on occasion, multinational corporations and the global population who "believe that the rule or institution has come into being and operates in accordance with generally accepted principles of right process."[50] As mentioned in the preceding section, "legitimacy" correlates with "compliance": the more States perceive a rule, institution, or regime as legitimate, the higher the likelihood of these rules and institutions effectively inducing States to fully comply with their provisions, even in the absence of effective international mechanisms for enforcement. However, when the norm, institution, or regime in question is non-binding and lacks coercive power, it must rely more heavily on perceived legitimacy as a basis of influence.[51]

The literature distinguishes between diverse types of legitimacy. The most prevalent distinction differentiates between normative or moral legitimacy, and sociological—also known as descriptive, popular, or rational—

48. Christopher A. Thomas, *The Uses and Abuses of Legitimacy in International Law*, 34 OXFORD JOURNAL OF LEGAL STUDIES 729, 731 (2014).

49. Thomas Risse, *Transnational Governance and Legitimacy*, in GOVERNANCE AND DEMOCRACY: COMPARING NATIONAL, EUROPEAN AND INTERNATIONAL EXPERIENCES 179 (Arthur Benz & Yannis Papadopoulos eds., 2006).

50. THOMAS M. FRANCK, THE POWER OF LEGITIMACY AMONG NATIONS 19, 24 (1990).

51. Daniel Bodansky, *Legitimacy in International Law and International Relations*, *in* INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS: THE STATE OF THE ART 321, 325 (Jeffrey L. Dunoff & Mark A. Pollack eds., 2013).

legitimacy.[52] Both perceptions can be evaluated by three cumulative legitimating effects.[53] The first, a *source-based legitimacy*, is authority-oriented, emphasizing the claim to authority to rule, to make decisions and enforce the law. The collective consent of States is a prerequisite but does not suffice.[54] In the absence of normative authority to rule, there is no normative and sociological legitimacy for decision-making.[55] The second, a *process-based legitimacy*, is procedural-oriented and focuses on accepted principles of the "right process," such as fairness, transparency, accountability, inclusiveness, representation, and expert participation. Such a process serves as a legitimating criterion that, by virtue of its presence and application, legitimates the norm, regime, or institution.[56] The third, *outcome-based legitimacy*, is performance-oriented, assessing the extent to which the outcomes meet the legitimate expectations from any given process associated with the norm, regime, or institution.[57]

Evaluating legitimacy may involve both normative and sociological perspectives, as well as consideration of each legitimating effect (source, process, and outcome). For a norm, institution, or regime to be considered normatively justified, and therefore legitimate, it must demonstrate that its source to claim authority is normatively justified, as well as its processes and procedures and their outcomes. Additionally, from a sociological standpoint, legitimacy is determined based on a broad perception by States—through

52. John Tasioulas & Guglielmo Verdirame, *Philosophy of International Law*, ¶ 4.1, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Summer 2022), https://plato.stanford.edu/archives/sum2022/entries/international-law/; *see also* Allen Buchanan & Robert O. Keohane, *The Legitimacy of Global Governance Institutions*, 20 ETHICS & INTERNATIONAL AFFAIRS 405 (2006); Bodansky, *supra* note 51; David Lefkowitz, PHILOSOPHY AND INTERNATIONAL LAW: A CRITICAL INTRODUCTION 98 (2020); James G. March & Johan P. Olsen, *The Institutional Dynamics of International Political Orders*, 52 INTERNATIONAL ORGANIZATION 943 (1998); Mattias Kumm, *The Legitimacy of International Law: A Constitutionalist Framework of Analysis*, 15 EUROPEAN JOURNAL OF INTERNATIONAL LAW 907 (2004).

53. C.A. THOMAS, THE CONCEPT OF LEGITIMACY AND INTERNATIONAL LAW 7 (Law, Society and Economy Working Paper, Dec. 2013), https://eprints.lse.ac.uk/51746/1/__libfile_repository_Content_Law,%20society%20and%20economics%20working%20papers_2013_WPS2013-12_Thomas.pdf; *see also* Bodansky, *supra* note 51, at 326–29.

54. Bodansky, *supra* note 51, at 330.

55. *Id.* at 329; *see also* Jonas Tallberg & Michael Zürn, *The Legitimacy and Legitimation of International Organizations: Introduction and Framework*, 14 THE REVIEW OF INTERNATIONAL ORGANIZATIONS 581, 586 (2019).

56. FRANCK, *supra* note 50; *see also* Daniel Bodansky, *The Legitimacy of International Governance: A Coming Challenge for International Environmental Law*, 93 AMERICAN JOURNAL OF INTERNATIONAL LAW 596, 602 (1999).

57. THOMAS, *supra* note 53, at 7; *see also* Bodansky, *supra* note 51, at 329.

examining the attitudes and beliefs of their government officials, populations, and other constituencies such as civil society NGOs—that a particular norm, institution, or regime is morally (normatively) authoritative.[58] The effectiveness of process or outcome normative legitimation depends on what produces good reasons for claims to authority. In contrast, the effectiveness of process or outcome sociological legitimation depends on what produces legitimacy beliefs.[59] That said, the widespread view is that legitimacy has both dimensions, normative and sociological, to varying degrees, based on the circumstances of each situation.[60] Moreover, the level of legitimacy "is a matter not of all or nothing, but of more or less."[61]

Franck specifies four interrelated properties to assess the legitimacy of rules and rule-making processes: "Determinacy" refers to the rule's clarity and transparency, and the accessibility of a designated process, to clarify a vague rule and how it should be interpreted and applied in given, contested instances;[62] "Symbolic validation" refers to rituals and regularized practices that ensure authentication;[63] "Coherence" refers to implementation that is consistent ("likes be treated alike") and coherent (guarantees that any "distinction in the treatment of 'likes' be justifiable in principled terms" that are widely acceptable);[64] "Adherence" refers to the hierarchy of rules—a vertical nexus between primary rules or obligations and secondary rules that identify the sources of the rules and define how they are to be legislated, interpreted, and applied.[65] Accordingly, "in practice, the legitimacy of a forum [international institution or regime] can be tested in the same way as that of a rule: by reference to the determinacy of its charter, its pedigree, the coherence of

58. Jeffrey A. Lenowitz, *On the Empirical Measurement of Legitimacy*, *in* POLITICAL LEGITIMACY: NOMOS LXI, at 293, 296–97 (Jack Knight & Melissa Schwartzberg eds., 2019); *see also* Bodansky, *supra* note 51, at 329; THOMAS, *supra* note 53, at 24–27.

59. Lenowitz, *supra* note 58, at 297.

60. Melisa Schwartzberg, *Introduction*, *in* POLITICAL LEGITIMACY*:* NOMOS LXI, at 1 (Jack Knight & Melissa Schwartzberg eds., 2019); *see also* Bodansky, *supra* note 51, at 327, 329 (explaining that although the two types of legitimacy differ, they are mostly intertwined).

61. Buchanan & Keohane, *supra* note 52, at 406; *see also* FRANCK, *supra* note 50, at 26 ("if legitimacy is a determinant of the strength of a rule's compliance pull, then legitimacy, too, must be a matter of degree"); Bodansky, *supra* note 56, at 624.

62. Franck, *supra* note 34, at 93–94; *see also* FRANCK, *supra* note 50, at 30, 52.

63. Franck, *supra* note 34, at 92, 134.

64. *Id.* at 144, 147–48.

65. *Id.* at 184.

its mandate and its adherence to the normative institutional hierarchy of international organization."[66] Implementing impartial mechanisms of accountability, transparency, and participation in crafting rules, and in governance, could reinforce the legitimating source, process, and outcome effects. The resultant rules and governance institutions would be widely viewed as just, or at least as more just, and thereby more legitimate, than those produced without such mechanisms.[67]

Our discussion on legitimacy in the context of regulating and governing cyberspace would not be complete without direct reference to important scholars' views regarding the legitimacy of international/global governance institutions.

Fritz Scharpf evaluates the legitimacy of democratic international governance institutions, in the context of the European Union (EU), using two criteria: *input legitimacy* and *output legitimacy*. Input legitimacy is a procedural-oriented legitimacy relying on due process, which includes fundamental democratic components such as transparency, accountability, and, more importantly, participation in the decision-making process to ensure "government *by* the people." In fact, it overlaps the source and process-based legitimacy discussed above. Output legitimacy is a substantive, outcome-oriented legitimacy that indicates the extent to which the EU's policy is effective and meets the expectations of "government *for the people*."[68] Scharpf argued that the EU lacks input legitimacy because it has little collective European identity while output legitimacy is "[*public*] *interest based rather than identity based*."[69] Vivien Schmidt suggests a third criterion, *throughput legitimacy*, which "is judged in terms of the efficacy, accountability and transparency of the EU's governance processes along with their inclusiveness and openness to consultation *with* the people."[70]

In his study on international governance, Daniel Bodansky indicates three categories to evaluate legitimacy.[71] The first, *democracy-based legitimacy*, stipulates that the authority of international governance relies on the volun-

66. Thomas M. Franck, *Legitimacy in the International System*, 82 AMERICAN JOURNAL OF INTERNATIONAL LAW 705, 725 (1988).

67. Lefkowitz, *supra* note 52, at 109.

68. FRITZ SCHARPF, GOVERNING IN EUROPE: EFFECTIVE AND DEMOCRATIC? 6 (1999).

69. *Id.* at 12.

70. Vivien A. Schmidt, *Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput'*, 61 POLITICAL STUDIES 2, 2 (2013).

71. Bodansky, *supra* note 56, at 612.

tary consent of States. This is a prerequisite but an insufficient one: implementing political equality based on a "one State, one vote" formula is problematic given the vast disparities in the democratic credentials of different States. Second, *participatory legitimacy* focuses on transparency and public or State participation in governance processes.[72] The degree of transparency and participation affects whether, and to what extent, the decision-making process would be perceived as legitimate. Although affording transparent and participatory processes might be challenging, it is still feasible through committees and working groups that would publish their agendas and provide interested stakeholders the opportunity to influence through active participation. A lack of multi-stakeholder participation and transparency would undermine procedural and substantive legitimacy (process-based and outcome-based legitimacy). Third, *expert legitimacy* focuses on involving relevant experts to provide decision-makers with professional, impartial, and independent analysis on the feasibility and effectiveness of each line of action. In sum, the following three cumulative conditions are essential to establish legitimacy to support international governance institutions or mechanisms: (a) The international institution should function in accordance with the law to ensure legal legitimacy, the source-based legitimacy (democracy-based legitimacy); (b) the decision-making mechanism or process should be transparent and should allow people and every State the opportunity to participate (participatory legitimacy); and (c) decisions should be based on the best scientific expertise (expert legitimacy). Although these components are essential to establish legitimacy, they do not suggest how decisions should be made when consensus cannot be reached.[73]

Allen Buchanan and Robert Keohane view the concept of legitimacy in global governance institutions through the lens of the right to rule. This means that global governance institutions are morally justified in forming the rules, States' consent is a prerequisite, and those States or populations have moral content-independent reasons to follow the rules and not to interfere with others' compliance with them.[74] The co-authors articulate a *Complex Standard of Legitimacy* for global governance institutions that includes the following suggested substantive criteria: (a) minimal moral acceptability—the global governance institutions are required to respect and safeguard the least

72. *Id.* at 617–19.

73. *Id.* at 624; *see also* Seita Romppanen, *The Role of Science in Regulating Sustainable Energy Democracy*, *in* SUSTAINABLE ENERGY DEMOCRACY AND THE LAW 54 (Ruven Fleming et al. eds., 2021).

74. Buchanan & Keohane, *supra* note 52, at 411.

controversial human rights, like physical security, liberty, and the right to subsistence; (b) comparative benefit—the global governance institution's legitimacy is justified when it is more effective than alternative institutions while also meeting the moral acceptability criterion; and (c) institutional integrity—actual performance should conform with the global governance institution's procedures and goals.[75] Additionally, the global governance institution must develop mechanisms to uphold accountability for meeting those substantive criteria and mechanisms to challenge the terms of this accountability. These mechanisms must be transparent, including by publicly explaining and justifying their main efforts, and making information about the mechanisms and their manner of function transparent and accessible.[76]

Allen Buchanan offers a *meta-coordination view* of legitimacy[77] that does not focus on the right to rule but serves a specific practical function, striving to invoke rules States and individuals can comply with out of an independent moral perception and not a duty to obey. The *Meta-Coordination View* does not require unanimity but a "workable consensus," a consensus of enough of those in a position either to facilitate or interfere with the functioning of the institution. Hence, an institution is legitimate if a workable consensus regards it as morally worthy and the benefits of empowering it outweigh the risks.[78] Moreover, such an institution can function without reliance on the threat of coercion or inducements of self-interest.

1. Implications for the List of Non-Binding Norms's Legitimacy

The universal consensus that underpins the List of Non-Binding Norms is not comparable to the consent granted by States when acceding to global treaties. Such treaties typically include binding provisions and may establish proper mechanisms for dispute settlement and verifying compliance. Unlike Allen Buchanan's concept of "workable consensus," which seeks to invoke uncontested norms that States uphold relying on a shared moral perception rather than a duty to obey, the UN-GGE 2013, 2015, and 2021 final reports[79] relied on an "enabler consensus." Without consensus, they would have collapsed. The P5, which had permanent seats in each UN-GGE, strove to meet

75. *Id.* at 420–23.

76. *Id.* at 427–28.

77. Allen Buchanan, *Institutional Legitimacy*, *in* OXFORD STUDIES IN POLITICAL PHILOSOPHY 53 (David Sobel et al. eds., 2018).

78. *Id.* at 54–55.

79. *See* sources cited *supra* note 13.

this challenge recurrently without incurring any significant political costs at the expense of their conflicting strategic interests. Therefore, they collaborated in creating the List of Non-Binding Norms as a voluntary, non-binding international instrument.

Moreover, the List of Non-Binding Norms includes indeterminate norms and lacks any methodology to provide authorized interpretation other than a new inclusive consensus to clarify, interpret, or render those norms or their interpretations into binding rules. Additionally, Franck's interrelated properties, as discussed above, are narrowly embodied, if at all, in the List of Non-Binding Norms. Determinacy and symbolic validation are deliberately absent from the List, creating inherent legal and legitimacy deficits that also severely affect and even preclude the remaining interrelated properties of coherence and adherence. States' reluctance to address these deficits and provide a higher degree of determinacy by eliminating normative ambiguities and resolving controversies related to interpretation and application, not to mention recognized norms of customary international law, perpetuates flawed legitimacy. This is evident from both the normative and sociological perspectives.

As a result, the legal and legitimacy gaps converge into a significant accountability gap, undermining the ability to hold States accountable for violating norms on the List of Non-Binding Norms. Thus, the List's source-based legitimacy is significantly limited. Furthermore, the legitimacy deficit extends to both process-based and outcome-based legitimacy within the UNGA resolutions reaffirming the List. None of these resolutions has established impartial, fair, and transparent mechanisms of accountability that integrate international expertise and State participation. There is neither an impartial authorized mechanism to apply norms of the List consistently and coherently, nor an international, independent mechanism to attribute State responsibility, including for violating norms of the List. Consequently, each State is sovereign to investigate, independently, every cyber attack targeting its network, and based on its own findings and national strategic considerations, attribute responsibility to the implicated State or entity. Implementing impartial international bodies authorized to coherently apply the List and to credibly attribute State responsibility would undoubtedly significantly strengthen the legitimating effects of the List's source, process, and outcome-based legitimacy.

Because of the lack of legal clarity described above, the List of Non-Binding Norms serves more as a reference for holding States accountable

for irresponsible behavior than specifying the legal responsibility for breaching any specific binding international rule. The United States and the United Kingdom have led the "Five Eyes" intelligence-sharing alliance—the United States, United Kingdom, Australia, Canada, and New Zealand—to embrace and implement a strategy of collective attribution and response, drawing on the outcomes of their national attribution processes. However, these processes possess characteristics that interfere with its legitimating effects and significantly impair its effectiveness and deterrence. The strategy's objective is to mold the List of Non-Binding Norms or derive from it "rules of the road" and deter States from violating these rules. However, as of yet, this has not been achieved.[80]

2. International Instruments to Hold States Accountable for Irresponsible Behavior in Cyberspace

Another way to reinforce State accountability and compliance with the List of Non-Binding Norms is through international alliances that aim to collectively delegitimize irresponsible State behavior, attribute responsibility, and deter by imposing costs, either through sanctions or offensive cyber operations that do not cross the threshold of use of force. If implemented transparently, consistently, and effectively, this approach could enhance the List's legitimacy and State accountability. The first attempt to establish such an international instrument on top of national attributions was the International Cyber Deterrence Initiative. The Trump Administration launched this within the U.S. 2018 National Cyber Strategy. Its main purpose was to deter States from violating the List of Non-Binding Norms through collective attribution and collective responses.[81] In fact, no State, including the United States' partners in the Five Eyes, has officially joined the International Cyber Deterrence Initiative. Ultimately, this initiative never took shape as an active international initiative.

80. For a full discussion of the collective attribution process and policy and their limitations, *see* Dan Efrony, *Collective Attributions in Cyberspace—A Rebranded Version of Attribution Does Not Make It More Effective*, 103 INTERNATIONAL LAW STUDIES 270 (2024).

81. THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (Sept. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

The second attempt was the Joint Statement on Advancing Responsible State Behavior in Cyberspace.[82] The United States, Australia, and the Netherlands co-sponsored this international initiative of twenty-eight UN member States in September 2019. This joint statement includes a commitment to hold States accountable for violating the List of Non-Binding Norms and to transparently impose costs in accordance with international law. The States joining this initiative have followed up on the statement only once. In February 2020, fifteen of the twenty-eight partner States joined forces with Georgia in attributing to Russia responsibility for a disruptive cyber campaign conducted by the Russian military intelligence agency. These States denounced Russia and called on it to comply with the List of Non-Binding Norms.[83] Since then, this initiative has never been invoked in the international discourse on applying international law or norms of responsible State behavior in cyberspace.

As indicated, both initiatives (International Cyber Deterrence Initiative and Advancing Responsible State Behavior in Cyberspace) have failed to garner any political significance and, in fact, have dissipated, making a negligible, if any, impact on the degree to which States view the List of Non-Binding Norms as legitimate or justify their compliance. Instead of these initiatives, the United States, along with its partners in the Five Eyes, has shifted focus to collective attribution as a means to internalize the List, which it considers as reflecting legitimate norms of responsible State behavior, as perceived by the attributing States. The aim is to enhance State compliance with these norms and bolster the List's perceived legitimacy, in conjunction with the deterrent effect of official attributions. Nonetheless, even this strategy, and its manner of implementation, have failed to make significant strides. Recent research suggests that its effectiveness may have been overestimated. Between 2017 and January 2024 the number of collective attributions reached just fourteen, and none of them could be considered a milestone in influencing State behavior in cyberspace or even the behavior of the States held accountable.[84]

---

82. Australia et al., Joint Statement on Advancing Responsible State Behavior in Cyberspace (Sept. 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ (The twenty-eight States issuing the statement included the Five Eyes, Japan, and Korea. The remaining States were EU members.).

83. *See, e.g.*, Press Release, U.K. Foreign & Commonwealth Office, UK Condemns Russia's GRU Over Georgia Cyber-Attacks (Feb. 20, 2020), https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (the British official statement).

84. For a detailed discussion of these fourteen attributions, *see* Efrony *supra* note 80.

Despite this, in October 2021 the United States launched a third international initiative, the International Counter Ransomware Initiative. Three consecutive ransomware cyber attacks originating in Russia had targeted American companies (Colonial Pipeline, JBS Foods, and Kaseya) causing large scale harm to U.S. national interests.[85] This might have been the final catalyst to the International Counter Ransomware Initiative's establishment. President Biden successfully used his first summit with his Russian counterpart to garner action against these Russian cyber attacks, which were launched from Russian sovereign territories. Biden set out American red lines regarding cyber attacks, accompanied by an unequivocal warning that crossing those lines would lead the United States to respond using America's "significant cyber capability."[86] Thus, the two leaders agreed on promoting understandings through a joint negotiation group whose first fruit was the UNGA Resolution, which unified the parallel UN tracks into one, under the Open-Ended Working Group.[87] Following this development, in January 2022 the Russian Federal Security Service (FSB) announced that it had raided and shut down the operations of the "REvil" ransomware gang, whose members were suspected of conducting the three aforementioned cyber attacks.[88] The Security Service detained and charged members of the gang. This unprecedented collaboration at the request of the U.S. authorities, together with the coordinated UNGA resolution, could have served as a clear sign of both sides' readiness to cooperate and compromise in resolving disparities, despite their strategic rivalry. However, the Russian invasion of Ukraine reshuffled the cards in this regard; the United States halted the ne-

85. Steve Holland & Andrea Shalal, *Biden Presses Putin to Act on Ransomware Attacks, Hints at Retaliation*, REUTERS (July 10, 2021), https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/ .

86. Vladimir Soldatkin & Steve Holland, *Far Apart at First Summit, Biden and Putin Agree to Step on Cybersecurity, Arms Control*, REUTERS (June 16, 2021, 8:47 PM), https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/.

87. G.A. Res. 76/19, *supra* note 15.

88. Page, *supra* note 16; *see also* Federal Security Service of the Russian Federation, *Illegal Activities of Members of an Organized Criminal Community Were Suppressed* (Jan. 14, 2022), http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html (as translated by Microsoft Edge browser translation service).

gotiation process, and the REvil Russian gang quickly sprung back into action.[89] Undoubtedly these developments reinforce the justification for establishing the International Counter Ransomware Initiative.

Although the Counter Ransomware Initiative focuses on specific criminally motivated cyber operations, its importance should not be underestimated.[90] Unlike the International Cyber Deterrence Initiative and Advancing Responsible State Behavior in Cyberspace, the International Counter Ransomware Initiative is specifically designed to counter ransomware cyber operations. The U.S. Administration has recently defined such criminally motivated cyber operations as a threat to U.S. national security.[91] The International Counter Ransomware Initiative centers its efforts on strengthening cooperation and fostering the exchange of information and professional expertise among States and incorporating the private sector. Collaboration with the private sector has the sole purpose of countering ransomware by building technical capacities to bolster resiliency and disrupt capabilities. The International Counter Ransomware Initiative has already established the International Counter Ransomware Task Force[92] to coordinate and disrupt ransomware at the operational level. This necessitates substantial cooperation, potentially involving capabilities to investigate and to attribute responsibility, yet primarily engaging in defensive or offensive cyber activities against hack-

89. TASS, *supra* note 16; *see also* Ravie Lakshmanan, *New REvil Samples Indicate Ransomware Gang is Back After Months of Inactivity*, HACKER NEWS (May 10, 2022), https://thehackernews.com/2022/05/new-revil-samples-indicate-ransomware.html (reporting about indications of REvil's revival).

90. Press Release, The White House, International Counter Ransomware Initiative 2023 Joint Statement (Nov. 1, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/ (Briefing on the key deliverables of the third annual gathering. The number of initiative members is growing each year, and as of November 2023, there are fifty members: forty-eight States, the EU, and INTERPOL).

91. THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 17 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

92. The White House, Fact Sheet: The Second International Counter Ransomware Initiative Summit (Nov. 1, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/ (statement on the decision to establish an International Counter Ransomware Task Force including twenty-seven participating States led by Australia as chair and coordinator of joint coalition work through sharing information and capabilities in the fields of resilience, disruption, and countering illegal financing).

ers detected in ransomware attacks, whether acting independently or on behalf of others, including States. Such cooperation could also include holding States accountable for ransomware cyber operations recurrently launched from within their sovereign territory. However, rather than meeting the legal challenges such accusations could entail, the International Counter Ransomware Initiative's States parties might prefer to hold States accountable for irresponsible behavior.

Yet, since its establishment, the International Counter Ransomware Initiative has not attributed responsibility to any State for ransomware attacks carried out by the State's proxies or official agents operating from its sovereign territory. This absence of attribution is likely due to strategic political considerations rather than inferior cyber investigative capabilities. In colloquial terms, it is a question of policy rather than ability.

3. A Vicious Cycle, Not a Dead End

In conclusion, the UN process described above achieved consensus among all competing powers for establishing the List of Non-Binding Norms as the normative layer for responsible State behavior in cyberspace. Unsurprisingly and deliberately, it is a voluntary, non-binding, ambiguous, and non-comprehensive normative layer. Thus, it is a weakened layer, which cannot be legally enforced; otherwise, consensus could have never been reached. In addition to the legal difficulties associated with this ambiguous normative layer, its source-based legitimacy—morally and sociologically—is limited, as are its process and outcome-based legitimacy. Furthermore, States supplement this normative layer through national attribution processes rather than through international, impartial, transparent, and professional mechanisms to interpret norms, investigate violations, attribute responsibility, and resolve disputes. In these circumstances, the legitimacy of the current arrangement—weak normative layer plus the national (mostly American) attribution process—remains low, as does its effectiveness. Given the enduring Great Power Competition, the conflicting strategic interests, and the fundamental mistrust among the competing powers, the international community has not yet reached, and seemingly will not reach—at least not in the near future—the desired universal consensus to fill major gaps and significantly enhance the normative layer. While the situation has reached a vicious cycle rather than a dead end—as the establishment of the International Counter Ransomware Initiative demonstrates—the next Part will delve into how this cycle might be resolved.

III. CONNECTING THE DOTS

Donald Mahley's quote cited at the opening of this article, which is more than two decades old, referred to biological threats escalated by significant scientific and technical innovations. Ambassador Mahley advised seeking an "outside the box" solution to verify State compliance with the Biological and Toxin Weapons Convention while rejecting a compromise draft protocol suggested by the chair of the Ad Hoc Group of States Parties. This proposed draft, known as the Composite Text, concluded seven years of negotiating an effective and legally binding verification regime for the Biological and Toxin Weapons Convention. It would establish a binding verification mechanism based on three pillars: declarations, on-site visits, and investigations within a compliance architecture like that of the Chemical Weapons Convention. The objection of the United States, the most influential power among the States parties, blocked the consensus required for approving the Composite Text. Ambassador Mahley claimed that its risks outweighed its benefits.[93] The U.S. objection relied on two categories of arguments: practical difficulties in applying verification procedures and potential risks to national security interests. Each is equally relevant to cyber tools and capabilities because of these similarities: (a) biological agents, like cyber components, are dual use technologies, accessible everywhere and to every individual expert, hub, or laboratory; (b) biological and toxin weapons, like cyber malwares, have the potential to pose enormous threats, spreading worldwide and causing formidable physical and indiscriminate damage; (c) both are strategically important, protected by confidential intellectual property and classified intelligence; and (d) the risks have become much more significant since non-State actors and individuals can develop, gain, or use the capability of producing biological and cyber weapons. As risks grow, States, notably Great Powers, are hesitant to expose their sensitive capabilities by cooperating with

93. Mahley, *supra* note 1; *see also* Marie Chevrier, *The Biological Weapons Convention: The Protocol That Almost Was*, *in* VERIFICATION YEARBOOK 2001 79, 79–97 (2001), https://www.vertic.org/media/Archived_Publications/Yearbooks/2001/VY01_Chevrier.pdf; FILIPPA LENTZOS, COMPLIANCE AND ENFORCEMENT IN THE BIOLOGICAL WEAPONS REGIME 17–19 (2019), https://unidir.org/files/2019-12/UNIDIR%20WMD%20CE%20-%20Paper%204%20v2.pdf; Jack M. Beard, *The Shortcomings of Indeterminacy in Arms Control Regimes: The Case of the Biological Weapons Convention*, 101 AMERICAN JOURNAL OF INTERNATIONAL LAW 271, 283–85 (2007).

an independent international compliance mechanism. This reluctance hinders their ability to effectively manage those risks, as the COVID 19 pandemic demonstrated.

Ultimately, the United States decided to object to the proposed Composite Text, considering it a useless, inefficient, and non-deterrent mechanism, and ruled out any option to modify it since "trying to do more would simply raise the risk to legitimate United States activities."[94] Consequently, the Biological and Toxin Weapons Convention functions with no compliance mechanism or measures except the UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons. This is not a standing body of investigation but rather ad hoc fact-finding teams that the Secretary-General is authorized to establish. To date, the Secretary-General has never done so in the context of biological weapons. In the context of chemical weapons, the Secretary-General has done so only three times, twice in 1992 and once in 2013.[95] However, every on-site investigation, either through the Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons or the Organization for the Prohibition of Chemical Weapons, regarding prohibited use of chemicals, requires pre-coordination with the concerned State.[96] This, in and of itself, is a considerable obstacle undermining any efficient and impartial investigation. The minuscule number of investigations held to date may speak for itself about the Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons's limited practicality and effectiveness, let alone if transplanted to an active digital battlefield in the under-regulated cyberspace, with its weakened normativity.

Yet this should definitely not discourage those who are determined to find a solution to ensure stability and security in cyberspace, including by reinforcing deterrence. On the contrary, it should primarily inspire a superpower like the United States to prevent the perpetuation of legal disparities and ambiguities concerning States' conduct in under-regulated cyberspace. The United States is simultaneously the leading and most influential power

94. *Id.*

95. U.N. Office for Disarmament Affairs, Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM), https://www.un.org/disarmament/wmd/secretary-general-mechanism/ (last visited Aug. 15, 2024).

96. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction art. VIII, Jan. 13, 1993, T.I.A.S. 97-525, 1974 U.N.T.S 45 (established the Organization for the Prohibition of Chemical Weapons (OPCW)).

in ensuring international order in cyberspace, while also being the State most vulnerable to politically, militarily, and economically motivated malicious cyber attacks. Furthermore, advanced cyber capabilities have become a game changer in every realm of life and domain, including the under-regulated outer space. While nuclear capability is not accessible legally and practically to every nation, and if used could be immediately detected and attributed to the responsible State, cyber capabilities are virtual, accessible to all, and hard to detect and legally attribute to the responsible State. States like China, Russia, Iran, and North Korea leverage this and the under-regulated cyberspace to threaten and indeed harm global stability, including by targeting U.S. national interests. On the whole, the risks of preserving a weakened normative layer and its negative impact on States' accountability and international order outweigh the national benefits of each State. This is a simple and direct response to "Franck's question" (here, presented as a non-rhetorical version): Why should a superpower like the United States "permit itself to be bound by norms and rules that may not always produce results that accrue to its advantage?"[97]

It is worth noting that the United States, along with its close allies, spares no resource in cooperating with dozens of States in establishing Cyber Emergency Response Teams (CERT), building their defensive capabilities, training and, if needed, even deploying American, British, and other allies' teams to assist in cyber defense and resiliency.[98] Moreover, investigating and attributing State responsibility may also prove hard in cyberspace, but still easier than in the biological realm, as noted above. Unlike the Composite Text, which requires on-site inspection, cyber investigations may be conducted remotely from outside the territory of the suspected culprit State. Additionally, from a national security standpoint, there is room, at times even a broad playing field, for flexibility in disclosing evidence.[99] The aforementioned International Counter Ransomware Initiative is an important initiative that illustrates such cooperation's potential to contend with one dangerous threat. However, by way of analogy, partially addressing one or two symptoms of a dangerous and contagious virus is insufficient to immunize the whole body against the diverse potential risks posed by that virus.

American leadership of a multinational effort is needed to break the vicious cycle and ensure a stable and secure cyberspace. However, any expectation of achieving a substantial and inclusive consensus, as inferred from

97. Franck, *supra* note 34.

98. Hunt Forward Operations, *infra* notes 118–121.

99. *See* discussion *infra* Part III(C)(2); *infra* text accompanying notes 170–172.

more than two decades of experience and the premises at the outset of this article, is futile. Nevertheless, given the intensifying cyber arms-race and cyber attacks within the Great Power Competition and recurring cyber "Pearl Harbors" and "wake-up calls," a consensus of the P5 is desirable, but it is not imperative and should not be perceived as such in bringing about the desired change. What I am proposing here is a new international legal framework that, on one side, enshrines invaluable normative clarity by removing ambiguities and resolving political and legal disputes related to the application of international law in cyberspace. On the other side, it establishes appropriate centralized international mechanisms to meet the essential challenges. What is crucial to accomplish this goal is what Allen Buchanan called a morally worthy "workable consensus."[100]

While it may not purport to achieve absolute inclusivity, this workable consensus should strive for significant inclusiveness by ensuring diverse representation from States, including cyber power States across all continents. Moreover, this consensus does not purport to address and resolve all contested political and legal questions. However, it is crucial for participating States to rise to the challenge of crafting an international convention that is both clear and sufficiently comprehensive. This would help convince as many States as possible of the genuine motive to serve global normative interests rather than the self-interest of any particular side. This workable consensus is crucial for establishing the major components of a reliable international legal framework. Despite the challenges, these interconnected elements—a workable consensus and international instruments (conventions, mechanisms, initiatives, etc.)—remain attainable.

Eventually, such a workable consensus would underpin a convention comprehensive enough to establish an international legal framework for cyberspace. This might include major components of binding rules, law enforcement, and cybersecurity mechanisms. The structure would consist of the following three elements (the "Triple I"): an International Cyber Law Convention (the Cyber Convention), which focuses on resolving the legal difficulties and discrepancies in regulating State behavior in cyberspace; an International Cyber Security Initiative, which serves as a global security regime or an international cyber security arm to enhance States' capabilities, accountability, and deterrence by bolstering interstate collaboration in implementing the rule of law and enhancing cybersecurity and resiliency; and an International Cyber Attribution Mechanism (the Attribution Mechanism),

100. Buchanan, *supra* note 77.

the "linchpin of accountability,"[101] which would provide high credibility and legitimacy to enhance accountability and guarantee effectiveness.

In the final stage, each of these components might constitute integral parts of the preferred comprehensive Cyber Convention. However, acknowledging the complexities and difficulties involved in establishing such a comprehensive and challenging convention and within a reasonable timeframe, it is preferrable for the international U.S.-led endeavor to achieve its goals in a modular and gradual manner, through multinational working groups (which may operate concurrently), with a plenary serving as the authorized body for final approvals. To be sure, the Cyber Convention is not a prerequisite for establishing the Attribution Mechanism and the Cyber Security Initiative. Both could be established independently based on a limited and focused workable consensus and could function in full cooperation and coordination. A salient success on the level of each of the two instruments, and notably the Attribution Mechanism, would serve as a confidence building measure to effectively influence achieving the workable consensus on the Cyber Convention's content and establishment.

The next three sections explore the three components, respectively. They are not in order of preference or feasibility. Section A addresses the question: Why is a Cyber Convention necessary, despite the lack of enthusiasm from the United States? Section B explores how the Cyber Security Initiative appears more practical and effective on its own and could be integrated or coordinated with existing initiatives. Section C delves into the Attribution Mechanism, which is prioritized as the first to be established as a centralized international mechanism, as soon as possible. Thus, the section is extended to explore various proposals for establishing such a mechanism, presenting recommendations and guidelines for overcoming the challenges entailed in establishing the Attribution Mechanism as a legitimate and credible mechanism.

A. An International Cyber Law Convention

As noted in Part II, the United States is the main opponent of the establishment of a new binding international treaty. The United States has been implementing an attribution policy striving to shape, case-by-case, what would constitute a breach of the List of Non-Binding Norms, and which norm of

101. JOHN S. DAVIS II ET AL., STATELESS ATTRIBUTION: TOWARD INTERNATIONAL ACCOUNTABILITY IN CYBERSPACE 49 (June 2, 2017), https://www.rand.org/pubs/research_reports/RR2081.html.

the List would relate to any given behavior. A previous study analyzing politically motivated cyber attacks conducted between 2012 and 2018 and a new study of the U.S.-led collective attribution strategy informed this policy.[102] Notably, the recent study has indicated that States, led by the United States and the United Kingdom, adopted a policy that applies norms of responsible State behavior instead of specifying international binding rules, in order to avoid narrowing their own operational leeway.

An International Cyber Law Convention might be an optimal alternative to the problematic normative layer discussed above, while augmenting the legality and legitimacy of the policy the United States and its close allies have been implementing. Such a convention would clarify how to interpret and apply to cyberspace the List of Non-Binding Norms and relevant international law norms and principles like sovereignty, due diligence, prohibitions on intervention, and use of force. Ideally, such a convention would also establish clear boundaries for legitimate acts of cyber espionage. Crossing these boundaries would constitute, at a minimum, a violation of sovereignty or a breach of new international rules prohibiting such cyber activities. In tandem, it would adjust and affirm the evidentiary standards applicable to cyberspace and might include an appropriate dispute settlement mechanism. It would also reconsider the suitability of countermeasures and adjust the legal requirements accordingly. In addition, it would contain updated definitions for use of force in cyberspace as the upper threshold for countermeasures and for a "cyber armed attack" to justify acts of self-defense against States and non-State actors.

Undoubtedly, the American arguments mentioned above,[103] explaining why a new treaty would be redundant or undesirable, were nothing more than unconvincing excuses for maintaining normative ambiguity to preserve operational leeway and the United States' qualitative edge. Interestingly, none other than Robert Hannigan, a former director of the United Kingdom's Government Communications Headquarters, expressed the opposite

---

102. Efrony & Shany, *supra* note 19 (when operating under conditions of significant normative uncertainty, States, and the United States as a major actor in the field, employ three interrelated strategies: "optionality"—regarding international law as an optional legal framework; "parallel tracks"—the development through State practice of formal rules backed by *opinio juris* and an informal set of rules shaped by practice without the sense of a legal obligation; and "gradations in law enforcement"—distinguishing between violations that are likely to lead to some form of response and those unlikely to do so); *see also* Efrony, *supra* note 80 (analyzing the findings of the U.S.-led collective attribution strategy and practice, as of January 1, 2024).

103. *See* Section II(A), *supra*; Markoff, *supra* note 33.

view just a few months after leaving office, stating: "We should be looking at some kind of arms control for cyberspace . . . *we do need to come to some kind of international agreement about what's acceptable and what isn't.*"[104] There are good indications for States' appetites to engage with other States in resolving existing disparities striving to reach an enhanced consensus that would safeguard the global public interest. Some of these indications are: the growing number of States, mostly Western, that have already published their *opinio juris* regarding multiple legal questions in cyberspace; the International Counter Ransomware Initiative already includes fifty participants (the EU, the INTERPOL, and forty-eight States from all continents);[105] seventy participants have thus far joined the Declaration for the Future of the Internet;[106] and fifty-four nations have already endorsed the Political Declaration led by the United States on Responsible Military Use of Artificial Intelligence and Autonomy.[107]

The Convention on Cybercrime (the Budapest Convention)[108] may serve as a model to follow. Despite its non-universality—the Council of Europe (CoE) initiated it—this document stands, thus far, as the only convention regulating international cooperation and criminal justice to suppress cyber crime. All the CoE member States (numbering forty-one at the time of negotiations in 2001) and four non-European States (the United States, Japan, Canada, and South Africa) participated in the negotiations stage to reach a consensus on a draft of a globally applicable convention. The Convention entered into force in July 2004. As of March 2024 seventy States have acceded to it.[109] Furthermore, a "large number of the remaining states have

104. Matt Burgess, *We Need a Global Cyberwar Treaty, Says the Former Head of GCHQ*, WIRED (Feb. 21, 2018), https://www.wired.co.uk/article/gchq-uk-robert-hannigan-cyberwar-definition (emphasis added).

105. International Counter Ransomware Initiative 2023 Joint Statement, *supra* note 90.

106. *See Declaration for the Future of the Internet*, U.S. DEP'T OF STATE, https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf (last visited Aug. 15, 2024).

107. U.S. Dep't of State, Bureau of Arms Control, Deterrence, and Stability, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/ (last visited Aug. 15, 2024).

108. Convention on Cybercrime, *opened for signature* Nov. 23, 2001, T.I.A.S. No. 13174, https://rm.coe.int/1680081561 (entered into force July 1, 2004) [hereinafter Budapest Convention].

109. As of March 14, 2024, twenty-two of the States parties are not members of the CoE. Additionally, there are twenty-three States with the status of observers—signatories that are invited to accede.

actually implemented the convention or parts of it, even if for political or other reasons some are not yet ready for accession."[110] A Cybercrime Convention Committee, whose plenary includes all States parties' representatives, functions as a steering committee for the convention and issues Guidance Notes aiming at "facilitating the effective use and implementation of the convention in the light of legal, policy, and technological developments."[111] When required, the committee also proposes to the CoE additional protocols with proper tools to meet new challenges raised by technological or political developments or controversies, which were intentionally left out of the Convention and now could be resolved by consensus.[112] Russia, which then was a CoE member State,[113] participated in the negotiations stage, but refrained from acceding to the Convention.

Almost two decades later, in 2019, Russia initiated a UNGA resolution to form an open-ended ad hoc intergovernmental committee of experts[114] in order to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. In doing so, it challenged the Budapest Convention. In a subsequent resolution, the UNGA decided that the ad hoc committee should accomplish its work by providing to the UNGA at its 78th session (in September 2024),

---

110. COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME: SPECIAL EDITION DEDICATED TO THE DRAFTERS OF THE CONVENTION (1997–2001), at 9 (Mar. 2022), https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e (testimonial of Henrik Kaspersen, who chaired the negotiating and drafting stage). For an indication of this quotation's accuracy, *see* Lennon Y.C. Chang, *Cybercrime and Cyber Security*, *in* COMPARATIVE CRIMINOLOGY IN ASIA 135 (Jianhong Liu et al. eds., 2017) (noting that the domestic laws of most ASEAN States are aligned with the main principles of the Budapest Convention, which provides a good basis for collaboration in countering cyber crimes).

111. *See, e.g.*, Cybercrime Convention Committee (T-CY), Guidance Note #11: Aspects of Terrorism Covered by the Budapest Convention (Nov. 15, 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bd640.

112. So far, the Budapest Convention has two additional protocols: Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, *opened for signature* Jan. 28, 2003, https://rm.coe.int/168008160f (entered into force Mar. 1, 2006); Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, *opened for signature* May 12, 2022, https://rm.coe.int/1680a49dab.

113. Council of Europe, Committee of Ministers, Res. CM/Res(2022)2 on the Cessation of the Membership of the Russian Federation to the Council of Europe (Mar. 16, 2022), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680a5da51.

114. G.A. Res. 74/247, Countering the Use of Information and Communications Technologies for Criminal Purposes (Dec. 27, 2019).

a draft convention.[115] However, after two years of negotiations, the concluding session held in February 2024 concluded with disagreement on fundamental points in the text of the draft treaty. Consequently, the committee decided to suspend the session and agreed to reconvene later to conclude its work within the original timeframe, subject to approval from the UNGA and the availability of financial resources.[116] As of the publication of this article, it remains to be seen whether the scheduled September 2024 session will prove conclusive.

These developments show that although the Budapest Convention is non-universal, it has had notable benefits; seventy States are active partners with close cooperation to implement the same technical and procedural measures for enforcing binding rules against cyber crimes according to Cybercrime Convention Committee commentary and guidance notes. Such consistent conduct by States parties may affect the conduct of other States while confronting cyber crimes. It may also play a significant role in shaping State practice in this field. Finally, its growth has become a catalyst for Russia and China to challenge the Budapest Convention in the UN arena. This may lead to the resolution of remaining controversaries by finding common ground or adopting a modus vivendi that each side can live with.

Although the proposed Cyber Convention does not aim to resolve every difficulty and settle all legal disputes at its initial stage, it would obligate its States parties to clearer and more accountable norms. Such an international convention would empower and legitimize States' accountability, even for non-party States. It would include binding norms that might limit cyber operations falling under the new normative framework. However, it would not necessarily restrict States parties from responding to States that have not yet acceded to the Cyber Convention and do not adhere to its provisions. This convention, if implemented on a broad and consistent scale, would significantly influence the shaping of State practice, which is a crucial factor in the development of customary international cyber law.

---

115. G.A. Res. 75/282, Countering the Use of Information and Communications Technologies for Criminal Purposes (May 26, 2022); *see also* Summer Walker, *Putting Pen to Paper*, GLOBAL INITIATIVE (Dec. 15, 2022), https://globalinitiative.net/analysis/un-convention-cybercrime-criminalisation/ (reporting about the draft convention that would be negotiated during the fourth session of the Ad Hoc Committee).

116. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft Decision Submitted by the Chair of the Ad Hoc Committee, U.N. Doc. A/AC.291/L.13 (Feb. 8, 2024), https://documents.un.org/doc/undoc/ltd/v24/008/21/pdf/v2400821.pdf.

B. An International Cyber Security Initiative

In June 2022, the head of the U.S. Cyber Command started publicly using the term "Hunt Forward"[117] instead of "Defend Forward." The commander of the Cyber National Mission Force, a Cyber Command unit that carries out offensive operations, described this activity as "one of the things we do on a daily basis"—targeting the tools needed for conducting attacks such as computers, internet connections, and malware.[118] Cyber Command officially claimed that it has been conducting "Hunt Forward Operations" since the 2018 midterm election campaign as an implementation of the "Defend Forward" strategy. Thus far, the Cyber National Mission Force has deployed fifty times and conducted hunt forward operations on over seventy-five networks in more than twenty-three States, at their invitation.[119] The United

117. Alexander Martin, *U.S. Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command*, SKY NEWS, (June 1, 2022), https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 ("General Nakasone confirmed for the first time that the US was conducting offensive hacking operations in support of Ukraine in response to the Russian invasion. He told Sky News: 'We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations.' The four star general did not detail the activities, but explained how they were lawful, conducted with complete civilian oversight of the military and through policy decided at the Department of Defence.").

118. Ellen Nakashima, *Cybercom Disrupted Russian and Iranian Hackers Throughout the Midterms*, WASHINGTON POST (Dec. 22, 2022), https://www.washingtonpost.com/national-security/2022/12/22/cybercom-russia-iran-attacks/; *see also* Cyber National Mission Force Public Affairs, *The Evolution of Cyber: Newest Subordinate Unified Command is Nation's Joint Cyber Force* (Dec. 19, 2022), https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=16012 ("According to Maj. Gen. William J. Hartman, the commander of CNMF, the sub-unified command designation reflects the success of CNMF in election defense, the Russia-Ukraine crisis, counter-ransomware operations, global hunt operations and support to thousands of operations of national significance."); Dina Temple-Raston, *Q&A with Gen. Hartman: "There are Always Hunt Forward Teams Deployed*", THE RECORD (June 20, 2023), https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here.

119. Press Release, U.S. Cyber Command, Cyber National Mission Force Public Affairs, *"Building Resilience": U.S. Returns from Second Defensive Hunt Operation in Lithuania* (Sept. 12, 2023), https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/; *see also* Posture of United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2025 and the Future Years Defense Program: Hearing Before S. Comm. on Armed Forces, 118th Cong., at 7 (Apr. 10, 2024), https://www.armed-services.senate.gov/imo/media/doc/20242.pdf (posture statement of General Timothy D. Haugh, Commander, U.S.

Kingdom followed suit in 2020 and established a similar unit—the National Cyber Force—which includes staff from the Government Communications Headquarters, MI6, and the Ministry of Defence. These operations disrupt "enemies physically, affecting supply chains and stopping malware or hacking attempts." According to the Government Communications Headquarters, all operations are "conducted in a legal and ethical manner, in line with domestic and international law."[120]

The strategy of countering cyber threats through global cyber operations in foreign territories is similar to the U.S. strategy of "zero tolerance" for terrorism.[121] The latter relies on U.S. legal authorization to deploy forces in foreign territories with the consent and cooperation of the local authorities to assist, train, and operate in countering terrorism. Regardless of the accuracy of this description, the pursuit of this undeclared policy for cyberspace cannot be sustained indefinitely, especially considering its lack of normative clarity and reliance on opaque criteria for holding States accountable. Furthermore, experience regarding the attribution process has also shown that the format of restricted cooperation with partners from the Five Eyes alliance and the EU is not a satisfactory solution.[122] Only a broad set of nations systematically working together in tandem and with sufficient transparency

---

Cyber Command, reporting that during 2023, Cyber National Mission Force personnel deployed twenty-two times to seventeen States to conduct Hunt Forward Operations); Nakashima, *supra* note 118.

120. U.K. National Cyber Force, *Guidance: Responsible Cyber Power in Practice* (Apr. 4, 2023), https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html; *see also* Lizzie Dearden, *UK Spies Waging Cyber-Attacks to "Weaken Adversaries" Including Russia and Iran*, INDEPENDENT (Apr. 6, 2023, 19:48 BST), https://www.independent.co.uk/news/uk/home-news/cyber-attacks-russia-uk-iran-gchq-b2313379.html.

121. GEORGE W. BUSH, NATIONAL STRATEGY FOR COMBATING TERRORISM 18, 23–24 (2003), https://irp.fas.org/threat/ctstrategy.pdf (President Bush calling all countries to adopt a "zero tolerance" policy for terrorist activity within their borders, comparing terrorism to slavery, piracy, or genocide and clarifying that "with our friends and allies, we aim to establish a new international norm regarding terrorism requiring non-support, non-tolerance, and active opposition to terrorists"); *but see* Renee de Nevers, *Imposing International Norms: Great Powers and Norm Enforcement*, 9 INTERNATIONAL STUDIES REVIEW 53 (2007) (discussing the role that force plays in changing international norms and concluding that when great powers seek to promote new norms, they will coerce the weak and keep persuading the strong).

122. Efrony, *supra* note 80.

to implement the List of Non-Binding Norms according to agreed legal interpretations can be conducive to international stability and can significantly shape State practice and enhance State accountability in cyberspace.

A study by Ethan Nadelmann that addresses the evolution of norms and global prohibition regimes identifies a common evolutionary pattern consisting of five stages.[123] During the first stage, most States do not yet consider the given activity as illegitimate, let alone unlawful. Thus, States could still be the perpetrators or enablers of such activities. During the second stage, international thought leaders, authoritative moral leaders, and legal scholars redefine the activity in question as evil. States that disregard this shift, either through direct actions by official organs, or indirectly by sponsoring or tolerating these actions by others, face gradual delegitimization. During the third stage, States capable of exerting hegemonic influence on a specific issue establish an international prohibition regime atop an international treaty. They subsequently encourage all States to collectively suppress the illegal activity. To succeed in establishing an effective global prohibition regime, these States may employ a wide variety of measures, including diplomatic pressure, economic inducements, military intervention, and information campaigns.[124] During the fourth stage, which is contingent on the success of the third, the global prohibition regime is up and running but it must contend with the challenges of antagonist States and weak States that may accede to the convention but are unable or unwilling to enforce its prohibitions within their territory. During the fifth stage, the scope of the prohibited activity is significantly reduced whereas the ability to use coercive actions against violations by States, entities, and individuals is limited. Furthermore, according to this study, despite the States' cooperation in enforcing the prohibitions, suppressing violations that have one or more of the following characteristics tends to be ineffective: easy to commit, easy to conceal, unlikely to be reported to the authorities, enjoys substantial consumer demand, and not easily replaced by alternatives. For this reason, the fight against drugs, for instance, has been ineffective compared to the more successful fights against piracy and the slave trade.[125]

---

123. Ethan A. Nadelmann, *Global Prohibition Regimes: The Evolution of Norms in International Society*, 44 INTERNATIONAL ORGANIZATION 479 (1990) (the study dealt with the evolution of the norms of piracy and privateering, slavery and the slave trade, extradition, international drug trafficking, "white slavery," and killing whales and elephants).

124. *Id.* at 484–86.

125. *Id.*

Transposing this evolving five-stage pattern to cyberspace reveals that, on the whole, the international community is still in the second stage of Nadelmann's scale. It may progress to the third and fourth stages by establishing the International Cyber Law Convention and enforcing its provisions through a centralized attribution mechanism and an International Cyber Security Initiative, as described below. As noted above, the Cyber Convention is not a prerequisite. The Attribution Mechanism and Cyber Security Initiative could be established independently based on a focused workable consensus. A salient success on this level, notably in bolstering the effectiveness of the List of Non-Binding Norms and enhancing accountability, would guarantee progress to the third stage.

However, on the level of countering pure cyber crimes, the international community could quickly advance to the third stage. Although the International Counter Ransomware Initiative described above[126] was originally designed to deal exclusively with ransomware, it could be extended to include additional cyber crimes and serve as a global prohibition regime atop of the Budapest Convention. Later, it could also rely on the new UN Cybercrime Convention—if it is approved and enters into force.[127] If pursued in this way, the International Counter Ransomware Initiative could be similar to another U.S. initiative—the Proliferation Security Initiative.[128] This was established atop of the Treaty on the Non-Proliferation of Nuclear Weapons[129] to interdict illegal shipments of materials related to weapons of mass destruction (WMD). The Proliferation Security Initiative's description as "a global initiative with an inclusive mission. . . . [A]n activity not an organisation," as well as the fact that it is not a binding treaty,[130] may also fit the International Counter Ransomware Initiative as a global prohibition or security regime.

---

126. *See* Section II(B)(2), *supra*.

127. U.N. Doc. A/AC.291/L.13, *supra* note 116.

128. *Proliferation Security Initiative for Searching Potential WMD Vessels*, 98 AMERICAN JOURNAL OF INTERNATIONAL LAW 355 (2004); *see also* U.S. Dep't of State, *About the Proliferation Security Initiative*, https://www.state.gov/proliferation-security-initiative/ (last visited Aug. 15, 2024).

129. Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, T.I.A.S. No. 6839, 729 U.N.T.S. 161.

130. U.S. Dep't of State, *Proliferation Security Initiative: Chairman's Conclusions at the Fourth Meeting* (Oct. 10, 2003), http://2001-2009.state.gov/t/isn/rls/other/25373.htm; *see also* AARON DUNNE, THE PROLIFERATION SECURITY INITIATIVE: LEGAL CONSIDERATIONS AND OPERATIONAL REALITIES (SIPRI Policy Paper No. 36, May 2013), https://www.sipri.org/sites/default/files/files/PP/SIPRIPP36.pdf; Duncan B. Hollis & Matthew C. Waxman, *Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI)*, 32 TEMPLE INTERNATIONAL & COMPARATIVE LAW JOURNAL 147 (2018).

Whether the new Cyber Convention is established or not, there is need to consider the establishment of an International Cyber Security Initiative as a global security regime designated to uphold a global cyber security or prohibition initiative through collaboration among States and with private security companies, academia, and civil society entities. The Cyber Security Initiative should endeavor to ensure: (a) nonproliferation of dangerous cyber technologies for terrorist organizations, criminal hackers, and irresponsible regimes;[131] (b) assistance to any member State in thwarting or countering serious disruptive or destructive cyber operations, including ransomware cyber operations; (c) sharing information, knowledge, expertise, and capabilities among States parties and with relevant entities from the private sector, civil society, and academia to enhance defense and resilience; and (d) development and implementation of technological features or changes in the network's protocols in coordination with relevant entities like the Internet Engineering Task Force, or the Internet Corporation for Assigned Names and Numbers. This may enhance cyber capabilities, including through AI, to detect anomalies, identify perpetrators, thwart malicious activity, and preserve evidence.

Existing international initiatives or arrangements, such as the International Counter Ransomware Initiative and CERT, could serve as significant foundations for such a centralized multinational body. Drawing from the experience of the United States and the United Kingdom with the establishment of the International Counter Ransomware Initiative and intensive multilateral cooperation within the framework of CERT and the like, it is reasonable to believe that establishing the Cyber Security Initiative is feasible even in parallel with the establishment of the Attribution Mechanism. Initially, the Cyber Security Initiative may focus on coordinating preventive cyber security measures or resilience efforts and on gathering evidence on probable violations of the List of Non-Binding Norms to transmit to the Attribution Mechanism. Like the Attribution Mechanism, the Cyber Security Initiative would also rely on achieving as wide a workable consensus as possible. Efficiency and effectiveness considerations would likely lead to merging the Cyber Security Initiative with the International Counter Ransomware

131. The International Cyber Security Initiative could help put institutional teeth into the Wassenaar Arrangement, whose scope has already been extended to include cyber tools that may be used to cause harm against States and human rights. *See* Innokenty Pyetranker, *An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement*, 13 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 153, 168 (2015).

Initiative, which currently focuses exclusively on addressing the ransomware threat, and to close collaboration and coordination with CERT, as well as with any other pertinent national security entities of the member States.

The legality of the Cyber Security Initiative should be evaluated by addressing the workable consensus that underpins its establishment and by appraising the answers to the following questions: Which international rules will the Cyber Security Initiative seek to enforce and to what extent will those rules be binding on the implicated State? What legal interpretations will be granted in this context to relevant legal principles such as jurisdiction, sovereignty, and due diligence, and to what extent will they reflect a workable consensus that would or might underpin the Cyber Convention? What would be the legal boundaries for cyber activities that this body is allowed to execute, and should such execution be contingent on the explicit consent of the States involved, either as victims or as the States from which the unlawful cyber action was launched?

C. An International Cyber Attribution Mechanism

The perceptions concerning the weakened normative layer in cyberspace and its diminished source-legitimacy, as well as the diminished legitimacy of the national attribution process and its outcomes, as discussed briefly in Part II of this article, have remained pertinent throughout the past decade.[132] Scholars, think tanks, NGOs, and private sector companies have dealt in recent years with the challenge of formulating proposals for new norms for cyberspace and how to ensure accountability and stability in cyberspace. This section reviews eight patterns of proposals. The focus is mainly on the question of how the international community can meet the challenge of establishing a credible attribution mechanism in cyberspace. Some of the proposals are quite general, based on the premise that the capacity to credibly attribute responsibility for unlawful cyber operations is a prerequisite for maintaining accountability. Some also include authority to adjudicate or settle disputes in addition to attribution power, while others emphasize the necessity for an adjudicative body.

The following paragraphs succinctly review these proposals, dividing the eight patterns into two groups: those that include State or governmental participation, which are presented first, and those that exclude it, presented at

132. For detailed discussion about collective attribution strategy and its low effectiveness, *see* Efrony, *supra* note 80.

the end of this section. There is also an internal division based on mechanisms that include dispute settlement and those that do not.

This overview of proposals is followed by an analysis and critique of their major pros and cons. Finally, guidelines are proposed for establishing a new and centralized attribution mechanism, which seeks to draw from the above analysis and from important insights about the legitimacy of international governance institutions, incorporating the best features of the previously proposed mechanisms, while avoiding their pitfalls. This will be presented in subsections 2 and 3.

1. Proposals for Meeting the Attribution Challenge

Proposals That Include State Participation

i. The Multilateral Cyber Attribution and Adjudication Council

A research team of the Atlantic Council suggested in 2014 the establishment of a council of governmental experts from cyber power States, like the P5, along with non-governmental experts from the private sector, academia, and civil society organizations.[133] The council of government experts would gather information from any relevant source, including States and the private sector, and would be designed to fulfill two complementary roles: to attribute responsibility for unlawful cyber operations and to settle related inter-State disputes. The council would be consensus driven. That would include requiring consensus on the determination of what international law is binding in cyberspace—the *de lega lata*. It would also require consensus in redefining lower evidentiary standards to enable attributing responsibility and issuing accompanying adjudicative decisions. If the council attributed responsibility, it would also be able to recommend steps to deescalate the malicious activity and rule on compensation. The Multilateral Cyber Attribution and Adjudication Council would transmit a full report, including the evidence and recommendations, to the UN Security Council, the International Court of Jus-

133. Jason Healey et al., *Confidence-Building Measures in Cyberspace: A Multistakeholder Approach For Stability And Security* 1–19 (Atlantic Council, Nov. 2014), https://www.files.ethz.ch/isn/185487/Confidence-Building_Measures_in_Cyberspace.pdf; *see also* Jason Healey, *Beyond Attribution: Seeking National Responsibility For Cyber Attacks* (Atlantic Council Issue Brief Jan. 2012), https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

tice, or a regional security council to consider undertaking additional enforcement actions. If the Multilateral Cyber Attribution and Adjudication Council failed, it would make that fact public and preserve the information it gathered for future use. The team expressed a belief that, by demonstrating its legal and technical competency, employing high security methodologies, and being impartial and transparent, the Multilateral Cyber Attribution and Adjudication Council would garner a high degree of legitimacy, encouraging States and private companies to cooperate.

ii. Incorporating Adjudication or Dispute Settlement Systems

This subcategory includes three proposals that focus on the adjudicative role:

1) *International Cyber Court or Arbitration*—A research team assembled by a Russian think tank[134] set a general plan to establish an effective cyber regime by consensus and cooperation among the major powers. In the short term (one year), States, along with the global technical community, would improve attribution technology and update core internet protocols to make the attribution process easier to conduct and increase effectiveness in verifying compliance with principles of international law. The mid-term (five year) objective would be to establish an international cyber court or arbitration mechanism. This platform would deal only with "government-level cyber conflicts" while independent experts would engage in verifying the accuracy of the evidence submitted by the involved parties. This task should be simpler and more reliable given the technological improvements implemented in the short-term stage. The long-term (ten year) objective would be to use the UN-GGE 2015 report as a starting point for establishing a binding UN convention on fighting cyber crime and a universal code of conduct for States in cyberspace.

2) *Court of Arbitration and Criminal Court*—Alexandra Perloff-Giles suggests a cyber arbitration forum under the 1958 New York Convention, like

134. Elena Chernenko et al., *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms: The Challenge*, COUNCIL ON FOREIGN RELATIONS (Feb. 23, 2018), https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms (working paper by three researchers from the Russian think tank "The Council on Foreign and Defense Policy").

the Court of Arbitration for Sport.[135] Such a forum could reside in the International Telecommunication Union, the Internet Engineering Task Force, or the Internet Corporation for Assigned Names and Numbers. This forum would allow civil accountability for transnational cyber offences. For transnational criminal law, Perloff-Giles recommends establishing a global agency, similar to INTERPOL, to develop digital forensics techniques and conduct investigations to support national prosecutions.[136] Alternatively, she suggests considering use of the International Criminal Court or a sui generis international criminal tribunal for cyber offenses, referring to the Draft UN Treaty on an International Criminal Court or Tribunal for Cyberspace, prepared by Stein Schjolberg, a former Norwegian judge.[137]

3) *An International Institution to Determine Accountability*—Rebecca Crootof suggests the creation of an independent international institution to determine accountability, namely, State liability for international cyber torts based on credible findings of an unbiased investigation.[138] This institution may also have the power to adjudicate and issue binding decisions on reparations and punitive damages. Naturally, it also may play a significant role in developing the law in cyberspace. In her view, such an institution would follow precedents like the International Atomic Energy Agency, the American Mexican Claims Commission, the UN Compensation Commission, the Iran-United States Claims Tribunal, and even the World Trade Organization.

iii. An International Cyber Regulatory and Attribution Agency

In 2016 Microsoft's research team proposed the establishment of an agency modeled on the International Atomic Energy Agency to verify compliance by States and private firms with cybersecurity norms proposed by another Microsoft research team.[139] The proposed agency would consist of highly

135. Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE JOURNAL OF INTERNATIONAL LAW 191, 211–14 (2018).

136. *Id.* at 214–15.

137. *Id.* at 222–23.

138. Crootof, *supra* note 32, at 637–39 (defining "international cyber tort" as "acts that employ, infect, or undermine the internet, a computer system, or a network and thereby cause significant transboundary harm" *id.* at 570).

139. Scott Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, MICROSOFT (June 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8; *see also* Angela McKay et al., *International Cybersecurity Norms: Reducing*

capable experts from governments, the private sector, academia, and civil society and would be representative, geographically and politically, to include, most notably, the P5. Thus, this proposal is also consensus driven. The agency would gather information from any relevant source, governmental or non-governmental. The main output would be transparent, as far as possible, and would include technical analysis of the cyber attack in question and the evidence that establishes technical attribution. The agency would base its authority on a high degree of credibility and legitimacy, as inferred from its structure, and the principles it upholds, such as transparency, expertise and multi-stakeholder participation. In addition, any attribution report would also be subject to peer review by relevant experts. Furthermore, to ensure effectiveness, the agency would address a small set of the proposed cybersecurity norms and would set a high threshold for a cyber attack's severity.

Scholars followed this line of thought, proposing the establishment of a new convention like the Chemical Weapons Convention and an international cyber security council,[140] a global cybersecurity regulatory agency,[141] or an independent organization to monitor and investigate transboundary cyber operations.[142] These scholars used the Organization for the Prohibition of Chemical Weapons as a model for the proposed enforcement arm. Like these scholars, Microsoft's President, Brad Smith, presented at the outset of 2017 a program that included the establishment of a new "Digital Geneva Convention" and the formation of a new international regulatory agency to investigate and identify States violating the convention. In addition, he suggested that key tech companies would jointly play a role similar to that of the Red Cross, playing "100 percent defense and zero percent offense."[143]

Conflict in an Internet-dependent World, MICROSOFT (2014), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA (suggesting six cybersecurity norms to limit conflict and a framework for developing additional proposed cybersecurity norms, by governments and the private sector).

140. Christina Lam, *A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election*, 59 BOSTON COLLEGE LAW REVIEW 2167, 2198–99 (2018).

141. Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 DICKENSON LAW REVIEW 1005 (2015).

142. Ido Kilovaty & Itamar Mann, *Towards a Cyber-Security Treaty*, JUST SECURITY (Aug. 3, 2016), https://www.justsecurity.org/32268/cyber-security-treaty/.

143. Brad Smith, President of Microsoft Corporation, Keynote Address at the RSA Conference 2017, The Need for a Digital Geneva Convention (Feb. 14, 2017), https://blogs.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

iv. Global Peer-Review Network for Cyber Attribution

In 2018 the "ICT4Peace" Foundation[144] offered an initial proposal to set up an independent network of experts from governments, the private sector, civil society, and academia to attribute factual-technical responsibility for wrongdoings in cyberspace.[145] Each participant would operate independently following standardized guidelines and submit their attribution results to a peer-review network. The idea was that if such a methodology of evaluation were used consistently, it would improve the attribution process's impartiality, thereby reinforcing trust and confidence in the process's results, and subsequently empowering the legitimacy of the attribution claim.

Proposals That Exclude State Participation

v. An International Cyber Attack Attribution Organization

In 2017 a Microsoft policy paper proposed the establishment of the International Cyberattack Attribution Organization, a non-governmental, non-political, private sector-led, and technology-focused attribution organization.[146] The organization would strengthen trust among multiple stakeholders in cyberspace by operating independently, transparently, and in political neutrality, to provide governments, enterprises, and the public with credible factfinding and a legitimate basis for further action. The organization would ensure organized and close cooperation with technology firms, maintaining a peer review process with diverse geographic representation. This approach assures that the final findings are objectively confirmed by a wide network of experts. The organization would investigate and attribute responsibility to

144. The ICT4Peace is a policy and action-oriented international foundation that is sponsored by and under the supervision of the Swiss Government. Its purpose is to use information and communications technology to save lives and protect human dignity by, inter alia, supporting the use of information and communications technology for peaceful purposes and promoting cybersecurity and a peaceful cyberspace. *See generally Mission*, ICT4PEACE, https://ict4peace.org/about-US/mission/ (last visited Aug. 15, 2024).

145. Serge Droz & Daniel Stauffacher, *Trust and Attribution in Cyberspace: A Proposal for an Independent Network of Organizations Engaging in Attribution Peer-Review* (ICT4Peace Foundation Cyber Security Policy Process Brief, 2018), https://ict4peace.org/wp-content/uploads/2019/07/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf.

146. *An Attribution Organization to Strengthen Trust Online* (Microsoft Policy Papers), http://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI (last visited Aug. 15, 2024).

culprit States for the most significant cyber attacks, according to a transparent threshold. While the proposed International Cyberattack Attribution Organization would be non-governmental, it would neutrally exchange information with governmental experts.

vi. An International Private Sector Attribution Organization

Like the International Cyberattack Attribution Organization proposal, a research team of the University of Washington's School of International Studies prepared in 2017 a detailed proposal for establishing a non-governmental attribution organization funded by the private sector and consisting of international experts from that sector and others.[147] The organization would include an expert investigation committee to investigate major State-sponsored cyber attacks, and an expert review committee, which would also include geopolitical academic experts, to assess the validity of attribution judgments. Both committees would adopt best practices of equitable geographic representation, organizational transparency, internal accountability, inclusion of technical and geopolitical experts, and private sector participation and collaboration with relevant international civil society organizations and tech and cyber security companies, including Chinese and Russian. Although the proposed organization would be non-governmental, it may receive government intelligence sanitized from sensitive items of information.[148] The committees would function under the oversight of the Executive Council of Company Representatives, which could veto attribution judgments by a majority of two-thirds of its members. The Council's members would serve under a four-year term limit to ensure diversity. The attribution report would be disseminated with full transparency to mainstream news organizations.

vii. A Global Cyber Attribution Consortium

In 2017 a research team operating within the RAND Corporation proposed the establishment of a Global Cyber Attribution Consortium for stateless

147. Justin Collins et al., *Cyberattack Attribution: A Blueprint For Private Sector Leadership*, at 26, HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES, UNIVERSITY OF WASHINGTON (2017), https://jsis.washington.edu/wordpress/wp-content/uploads/2017/07/ARP-2017-Report-FINAL.pdf.

148. *See, e.g.*, *id.* at 47 n.101 (citing "'Intelligence Community Directive 209-Tearline Production and Dissemination' (Office of the Director of National Intelligence, September 12, 2012)").

attribution to ensure neutrality and independence.[149] Only private companies and independent organizations would participate in establishing, funding, and operating the Attribution Consortium, at least until it gained a proven reputation as a trusted and credible international institution whose focus would be on public, and not legal, attribution. Therefore, the evidentiary standards would not be the same as those required in court. Furthermore, the Consortium's authority and legitimacy would stem from its reputation, relying on a high degree of credibility gained by the technical expertise of its diverse global and non-State membership and its commitment to objectivity and transparency. The Consortium would include a few dozen expert members while ensuring global representativeness, technical competency, and diversity of expertise. The investigatory process would be transparent regarding the methodologies it applies in selecting the incidents for investigation as well as collecting and evaluating the information. Furthermore, the Consortium would communicate its final findings to the relevant parties, providing them with the opportunity to be heard before publication.[150]

viii. Transnational Attribution Institution

The Internet Governance Project, in cooperation with Citizen Lab/University of Toronto, has proposed a Transnational Attribution Institution Working Group, a multi-stakeholder-oriented collection of university-based organizations and independent researchers that seeks to facilitate a transnational, independent, and neutral attribution process.[151] The Group's objective was to build a proposal for a Transnational Attribution Institution. Milton Mueller, who led this initiative in 2019, was inclined to exclude States and private companies from this idea, to ensure pure neutrality. Although Citizen Lab has not ruled out cooperation with tech platforms like Microsoft

149. DAVIS II ET AL., *supra* note 101.

150. *Id.* at 16.

151. Milton Mueller et al., *Cyber Attribution: Can a New Institution Achieve Transnational Credibility?*, CYBER DEFENSE REVIEW 107, 110 (Spring 2019), https://digitalmedusa.org/wp-content/uploads/2021/08/Badiei-Attribution-.pdf. For a summary of a conference on the article's content, *see* Farzaneh Badii, *Cyber Deterrence and Cyber Attribution: A Georgia Tech/Aspen Institute Event*, INTERNET GOVERNANCE PROJECT (June 3, 2019), https://www.internetgovernance.org/2019/06/03/cyber-deterrence-and-cyber-attribution-a-georgia-tech-aspen-institute-event/.

in investigating human rights abuses by cyber tools,[152] it tends to discourage this. As of yet it seems that the idea has not yet been translated into a concrete proposal.

ix. Conclusion

Naturally and justifiably, each of these proposals focuses on ensuring the credibility and legitimacy of the attribution process or mechanism, and its outcome, by embracing and integrating principles such as transparency, expertise, independence, and impartiality in the proposed mechanism, its structure, methodologies, and diversity of participants (sectors, expertise, States, and regions).

Four of the reviewed proposals exclude State engagement, allegedly to eliminate political bias, as this could erode the credibility of the attribution process and its outcomes. One of the four, which remains at the concept stage (Transnational Attribution Institution), tends to also exclude private sector engagement, focusing solely on academia and civil society organizations. The idea of ensuring impartiality by excluding States or private companies from the international attribution process is undesirable and unlikely to be effective, if at all feasible. Impartiality is not achieved by excluding essential partners whose contribution to revealing the truth is invaluable. Instead, it should be pursued by increasing the diversity of nationalities, competencies and expertise. This would help ensure impartiality and eliminate improper influence, thereby guaranteeing a highly credible process. Two detailed proposals (the Multilateral Cyber Attribution and Adjudication Council and the International Cyber Regulatory and Attribution Agency) address the lack of clear primary rules and evidentiary standards. Both proposals suggest lowering the legal requirements to correspond with the challenges of attributing responsibility in cyberspace. Otherwise, these requirements could be unattainable and stand as an insurmountable barrier to determining attribution. As explained below, if the Attribution Mechanism is established separately from the Cyber Convention, while the main legal difficulties remain pending, it would still be able to provide credible attributions.

152. Sam Levin, *Israeli Spyware Firm Linked to Fake Black Lives Matter and Amnesty Websites*, THE GUARDIAN (July 15, 2021), https://www.theguardian.com/technology/2021/jul/15/spyware-company-impersonates-activist-groups-black-lives-matter.

Unsurprisingly, the Russian think tank's proposal overlooks the legal challenges and coincides with Russia's cyber diplomacy as realized during the last decade. The short and mid-term objectives focused on substantiating the attribution determinations through technological evidence that should be openly examined through adversarial proceedings in court or arbitration. The long-term objective of establishing an international cyber crime convention and a universal code of conduct for States have already been major components in Russia's cyber diplomacy strategy. Thus, the UNGA approved a Russian proposal and assigned a UN ad hoc committee to formulate a UN international cyber crime convention.[153] In addition, Russia has already submitted to the Open-Ended Working Group its updated Concept of Convention for inclusion on the working group's agenda.[154]

Alas, all proposals have remained theoretical, apparently because of three cumulative reasons. First, proposals that require State participation are contingent on P5 consensus, which is currently impossible to achieve. Second, as experience hitherto shows, for successful attribution, it is essential for States to contribute through their intelligence and investigative entities. However, this contribution is often limited because these entities are reluctant to share their classified intelligence with foreign counterparts, fearing it may compromise intelligence sources and expose classified capabilities.[155] Third, Stateless international attribution mechanisms discourage States from cooperating and eventually also deter States from aligning with the outcomes of these mechanisms.

2. Centralized or Decentralized Model

Although the various proposals above were published between 2012 and 2019, none has progressed beyond the concept stage. Thus far, none of the cyber power States have publicly expressed its support or opposition regarding the question of whether a central, international attribution process or mechanism should substitute or supplement the attribution process currently in use, with its decentralized and non-standardized features. However, due to national security considerations of confidentiality and the Great Power Competition, the United States and the United Kingdom have shaped

153. G.A. Res. 74/247, *supra* note 114; G.A. Res. 75/282, *supra* note 115.

154. Press Release, Ministry of Foreign Affairs of the Russian Federation, *supra* note 31.

155. Burgess, *supra* note 104 (citing the former head of Government Communications Headquarters).

the current decentralized process, prioritizing coordination and information sharing, primarily within the framework of the Five Eyes, over any joint multinational mechanism of investigation and attribution.

Yuval Shany and Michael Schmitt suggest two arguments against replacing the current process.[156] The first is redundancy. Cyber power States are capable enough to efficiently investigate, attribute, and respond to a given cyber attack, while safeguarding their own national security interests. When needed, they can also collaborate with close allies and relevant firms from the private sector. While an independent international mechanism would bring legal clarity, it would exacerbate the asymmetry between cyber power States committed to the rule of law and their adversaries that lack any similar commitment. By reducing or removing legal ambiguity, cyber power States would lose the operational flexibility they currently maintain in determining whether to officially attribute and respond—when, where, and how—while safeguarding their national interests. As for the United States, keeping the current process in place serves the national security interest of maintaining supremacy over its rivals, Russia and China. The second argument is against establishing a new international treaty for cyberspace that would include a centralized international attribution mechanism as a major component for verifying and enforcing compliance. Kristen Eichensehr addresses this argument, suggesting that although a new central international attribution entity may be beneficial to credibly determine attributions, establishing such a mechanism is difficult and might be impractical. This is due to geopolitical divisions, constraints on the availability of all-source intelligence, and the limitations on resources for conducting an unlimited number of investigations.[157] Thus, she suggests that a centralized model should be developed in addition, and not as a substitute for, the prevailing decentralized model, which "decentralized and messy though it is, has some underappreciated virtues—ones that counsel in favor of preserving some multiplicity of attributors even alongside any future attribution entity."[158]

---

156. Yuval Shany & Michael N. Schmitt, *An International Attribution Mechanism for Hostile Cyber Operations?*, 96 INTERNATIONAL LAW STUDIES 196 (2020) (summarizing the findings and conclusions of a research project focusing on the need and feasibility of establishing an international attribution mechanism—I participated in that working group).

157. Kristen E. Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA LAW REVIEW 520 (2020).

158. Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 213 (2019) (an attribution organization might supplement and even strengthen currently disaggregated attribution efforts).

Nicholas Tsagourias and Michael Farrel express a skeptical view on whether a demanding set of conditions can ever be satisfied to ensure that a centralized international attribution agency would indeed be independent, professional, and impartial.[159] Their skepticism also encompasses States' willingness to cooperate with such an agency and comply with findings and determinations that they cannot independently scrutinize. Therefore, the authors concluded that creating an independent, impartial, and effective international agency for attribution in cyberspace is not so feasible and "quite premature," just adding "another layer in the already fractured attribution process."[160]

By contrast, other scholars,[161] and most of the proposals, recommend promoting a centralized governance approach to international cybersecurity challenges by following the model of confronting threats relating to WMD through intergovernmental organizations like the Organization for the Prohibition of Chemical Weapons and the International Atomic Energy Agency. Ido Kilovaty and Itamar Mann, for instance, emphasize that such a model would have a representative structure and decision-making processes that would preclude the option of being monopolized by any one superpower. In their view, such a treaty-based organization would not harm the United States, which would know how to maintain the required flexibility in employing its significant cyber capabilities when needed for self-defense. Nevertheless, disregarding the essential need for global cybersecurity governance by such an organization poses a risk to the national security of all States, including the United States.

Rebecca Crootof proposes the establishment of an independent and impartial international institution to determine State accountability or liability based on credible findings of an unbiased investigation of harmful or intrusive cyber operations.[162] In her view, an independent investigative institution with the appropriate expertise might help reduce disparities between States with varying levels of technological capabilities, making it better positioned to provide credible findings. Furthermore, its binding determinations might

159. Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 EUROPEAN JOURNAL OF INTERNATIONAL LAW 941, 959–61 (2020).

160. *Id.* at 961.

161. *See, e.g.*, Lam, *supra* note 140; Bagdasarova, *supra* note 141; Kilovaty & Mann, *supra* note 142.

162. Crootof, *supra* note 32.

contribute to the development of international cyber law, particularly in the context of State responsibility.

Martha Finnemore and Duncan Hollis opine that credible reports by an impartial international attribution organization could be a catalyst for States to coalesce around new international rules. In addition, States that lack cyber capacity could also benefit from such an organization and its technical expertise.[163] William Banks echoes this view.[164]

Shany and Schmitt argue that the need for a centralized, independent international attribution mechanism is still "viable and valuable" in cyberspace. An impartial, professional international institution "could lead to attribution determinations enjoying a higher degree of legitimacy."[165] The coauthors point to three constituencies that could benefit from such a new institution: "States with limited technological, intelligence, and diplomatic capacity; States interested in generating broad collective attribution of attacks perpetrated against them; and international and regional organizations operating a cyber-related sanctions regime."[166]

Undoubtedly, a new Cyber Convention is vital for strengthening the normative layer by removing ambiguities and resolving contested legal disputes. It is also essential for enhancing State accountability through a recentralized, independent, transparent, and impartial Attribution Mechanism whose main purpose is to impartially investigate cyber incidents and credibly hold States accountable for their wrongdoings. However, as noted above, assuring a workable consensus of States on establishing a comprehensive new Cyber Convention is a far-reaching and time-consuming task. Therefore, it would be inevitable to implement the proposal in stages, in a modular manner. At first, the objective would be to negotiate a treaty or an international initiative,[167] arrangement,[168] or the like, focusing merely on establishing an Attribution Mechanism. Later, it might be combined as an integral component of a broader, comprehensive cyber law convention. A workable consensus is a

163. Martha Finnemore & Duncan Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 EUROPEAN JOURNAL OF INTERNATIONAL LAW 969, 1002 (2020).

164. William Banks, *Cyber Attribution and State Responsibility*, 97 INTERNATIONAL LAW STUDIES 1039, 1071 (2021).

165. Shany & Schmitt, *supra* note 156, at 221–22.

166. *Id.* at 222.

167. Hollis & Waxman, *supra* note 130.

168. *See, e.g.*, Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Initial Elements, adopted by the Plenary of July 11–12, 1996, as amended by the Plenary of Dec. 6–7, 2001.

prerequisite for both. The United States, Five Eyes States, and EU member States constitute the natural core partners for such a consensus. They should extend it to include as many States—developed and developing—as possible, from all global regions.

Nevertheless, one might argue that establishing the Attribution Mechanism prior to resolving the open-ended legal questions is problematic since both are interrelated. I would claim the contrary. A centralized international institution, even when established prior to the Cyber Convention, has three important advantages. First, due to its expected structural properties, procedures, and methodologies—which are multinational, professional, impartial, independent, transparent, and peer-reviewed—it would be more credible and legitimate than any existing national attribution process. Therefore, the effectiveness of applying the List of Non-Binding Norms to attain States' compliance would be expected to increase as well. Furthermore, it might encourage States to retaliate more significantly and consistently than previously. Second, legitimizing the Attribution Mechanism's authority to make decisions according to both normative and sociological legitimacy perspectives would buttress the weight given to its decisions and consequently also its recommendations. Over time, these decisions would persuade an increasing number of States to align with views and recommendations they previously hesitated to embrace. Putting it more accurately, States' participation in such an impartial process would ensure that the Attribution Mechanism's attribution reports and recommendations on how to clarify and apply specific norms in cyberspace would fall on attentive ears and be implemented in State practice and integrated in the anticipated Cyber Convention. Third, a functioning Attribution Mechanism could also serve as a major confidence-building measure strengthening trust among the following constituencies: States parties to the Attribution Mechanism treaty (the first and limited version); States participating in the negotiations process to draft the Cyber Convention (the comprehensive version); States that remain outside the process, waiting to see how it develops; any relevant international governance organizations (regional, technological, law-enforcement, human rights); and the private sector, civil society, and academia. Undoubtedly, if such a mechanism were to be established and function in a manner that leaves no room to question its legitimacy and credibility, its attribution determinations would be more effective in applying the List of Non-Binding Norms and enhancing

States' compliance correspondingly.[169] It would also be an important catalyst to successfully accomplish the Cyber Convention project.

The International Cyber Attribution Mechanism, as a centralized international body, would not take over the role of the national law enforcement and intelligence agencies that currently constitute the decentralized attribution model. These governmental entities would not be rendered exempt from their national duties to investigate cyber attacks and identify their perpetrators. More significant and invaluable would be genuine collaboration by States and companies with the Attribution Mechanism by facilitating regular access to available knowledge, expertise, information, and even intelligence, though there may be occasions when access is circumscribed, as explained below. To ensure effective and efficient collaboration, the Attribution Mechanism would maintain permanent channels of communication with cooperative States and major private sector companies—tech platforms and cybersecurity firms. Moreover, since the Attribution Mechanism would not purport to investigate every cyber attack, States would be able to apply to the Attribution Mechanism to investigate cyber attacks they have already investigated, or are currently investigating, to leverage the Attribution Mechanism's credibility to enhance the legitimacy of the independent attribution determination made by these States. In sum, just as the Organization for the Prohibition of Chemical Weapons, the International Atomic Energy Agency, and the like have not obviated the role of national investigative entities, the establishment of the Attribution Mechanism would not make the national attribution processes redundant—quite the opposite.

Furthermore, another argument that may have an immediate restraining impact on the idea of a centralized International Cyber Attribution Mechanism stems from the following statement by a former Government Communications Headquarters Director: "Western governments could not trust the intelligence behind their assessments to an international body without compromising it."[170] This statement obviously makes sense and applies equally to the suspected State trying to dismiss accusations. However, controlling the risk of compromising sensitive intelligence interests is a manageable task, notably when the interest in balance is important enough. Embracing a sweeping approach to the treatment of classified intelligence information is aberrant and implausible. As a general rule, the ultimate decision on whether to disclose classified intelligence information and the extent of disclosure

169. Raustiala, *supra* note 37, at 425.

170. Burgess, *supra* note 104.

rests exclusively with the information's provider, contingent upon a calculation of potential gains and losses.[171] There is no wheel that needs reinventing here. Intelligence powers like the United States and the United Kingdom are skilled at meeting the challenge of protecting national security interests. This can be achieved by simply refraining from any overt or covert response that might compromise sensitive intelligence assets and interests, while allowing credible attributions and proper retaliations to effectively deter outlaw States and non-State actors. More familiar is the option of using proxy information, paraphrased information, and sanitized information instead of raw classified evidence that could put sensitive assets at risk of exposure.[172] This practice is in regular use by every intelligence agency and is included in the binding dissemination rules that dictate criteria, conditions, and restrictions for disseminating intelligence information and products to a wide range of recipients, including foreign governments and international organizations.[173] The wider the scope of dissemination, the lower the sensitivity of the intelligence released.

The challenge of establishing and activating the Attribution Mechanism is great, but it is worth the effort and is feasible, provided the United States is convinced and determined to pick up the gauntlet. Yet, it would still have to withstand scrutiny regarding the following three interrelated questions: Is the workable consensus that underpins the Attribution Mechanism broad

171. Florian J. Egloff & Max Smeets, *Publicly Attributing Cyber Attacks: A Framework*, 46 JOURNAL OF STRATEGIC STUDIES 502, 510–12 (2023). For additional readings about intentional disclosure of intelligence, *see* Ofek Riemer, *Politics Is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States*, 42 CONTEMPORARY SECURITY POLICY 554 (2021); Ofek Riemer & Daniel Sobelman, *Coercive Disclosure: The Weaponization of Public Intelligence Revelation in International Relations*, 44 CONTEMPORARY SECURITY POLICY 276 (2023); Shlomo Shpiro, *The Media Strategies of Intelligence Services*, 14 INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE 485 (2001).

172. *See, e.g.*, Director of Central Intelligence, DCID 1/7, Security Controls on the Dissemination of Intelligence Information (July 12, 1988) (¶ 7(b), concerning intelligence dissemination to foreign governments, permits the inclusion of intelligence information in reports provided to foreign governments provided, "The information is extracted or paraphrased to ensure that the source or manner of acquisition of the intelligence is not revealed and cannot be deduced in any manner.").

173. *See, e.g.*, Department of Defense, DoD Directive 5240.01, DoD Intelligence Activities (incorporating Change 3, effective Nov. 9, 2020) (Sec. 4.5.2: "The broadest possible sharing of intelligence with coalition and approved partner countries shall be accomplished unless otherwise precluded from release by law, explicit direction, or policy." Sec. 4.5.3: "Original classifiers shall draft intelligence products with a presumption of release and in such a manner as to allow the widest dissemination to allies, coalitions, and international organizations.").

and representative enough? To what extent are the leading cyber power States—most essentially, the United States—ready to be more transparent and incrementally withdraw from the policy of normative ambiguity in cyberspace? And, to what extent can the new institution deliver a genuine and steady message of legitimacy and credibility through its practice, structure, personnel, principles of action, and methodologies? These questions could be partially answered through the signing of the Attribution Mechanism treaty and how it has been structured and operated. Answers could also be derived from analyzing States' conduct, to the extent they and leading companies are cooperative and collaborate with Attribution Mechanism demands.

3. Suggested Guidelines for Establishing a Legitimate International Cyber Attribution Mechanism

As noted, the starting point is a substantial workable consensus among a wide and representative range of States on establishing International Cyber Attribution Mechanism—a centralized international governance institution—through a binding international agreement. That said, the following comments do not purport to provide States with a detailed plan of action. Rather they may serve as non-exhaustive guidelines for establishing the Attribution Mechanism with characteristics designed to ensure and reinforce the legitimating effect in its source, process, and outcomes.[174] This would ultimately yield a tangible legitimacy, both normative and sociological, that even external observers, who are not yet States parties, could not ignore. The seven suggested guidelines are as follows:

i. A Multi-Stakeholder Mechanism

It would be inconceivable for the Attribution Mechanism to be a government-free body. There are other ways, less drastic and far more effective, to assure impartiality, some of which are succinctly mentioned below. The Attribution Mechanism as a global governance institution would not replace the role of the national law enforcement and intelligence agencies. These would remain bound to their national duties to detect, investigate, and identify perpetrators. States' collaboration with the Attribution Mechanism,

174. *See* discussion *supra* Section II(B) and the relevant accompanying references regarding legitimacy.

through their professional governmental agencies, including by providing experts and intelligence to the Attribution Mechanism's investigative teams, would reiterate their commitment to the Attribution Mechanism's outcomes and be invaluable to its success.

ii. Transparent Criteria

The International Cyber Attribution Mechanism should develop well-defined transparent criteria for selecting cases for investigation or receiving cases by referral of victim States, either States parties or non-parties to the Attribution Mechanism treaty. The Attribution Mechanism's Executive Board would set and approve those criteria and would have the authority to decide on exceptional cases. Nevertheless, it is safe to assume that victim States with limited investigative capabilities to generate accountability on their own would refer relevant cases to the Attribution Mechanism. Similarly, more capable States may have an interest in attributing responsibility by an international centralized institution to gain more credibility and legitimacy.[175] Once the case is referred, the victim State would be expected to fully cooperate with the Attribution Mechanism, sharing information and intelligence up to the level of classification that its internal procedures allow (and that may change on a case-by-case basis). Should a victim State refer a cyber attack to the Attribution Mechanism for investigation and, in parallel, continue its own domestic investigation, the State would be expected to coordinate with the Attribution Mechanism any attribution determination it reaches and decides to officially announce. The goal of this coordination would be to afford quality assurance by reexamining the process if the findings of the investigative bodies are misaligned.

iii. Structure and Methodologies

The International Cyber Attribution Mechanism's structure and major methodologies would incorporate the following principles:

a) *Impartiality*—The Attribution Mechanism's investigative teams should independently make their own professional decisions with no external intervention. Their expert personnel should be multinational (from the

175. Shany & Schmitt, *supra* note 156, at 209.

Attribution Mechanism's States parties) and representative, and not necessarily consensus driven.

b) *Diversity of expertise*—This might encompass know-how that is governmental and non-governmental, including but not limited to cyber security, computer engineering, intelligence, and law. The Attribution Mechanism's experts must be extremely cautious and double-check the credibility of any piece of information to detect or preclude any attempt to deceive or mislead the investigation.

c) *Permanent procedures*—The Attribution Mechanism would establish permanent procedures including unified nomenclature and agreed probability yardsticks to evaluate the credibility of all evidence. The Attribution Mechanism would share these professional methodologies with its partners and counterparts among States and the private sector.

d) *Transparency*—The Attribution Mechanism would require transparency to the greatest extent possible, in full coordination with the classified information's providers, which could be governmental law enforcement organizations, intelligence agencies, tech platforms, cyber security firms, and even whistleblowers.

e) *Quality Control*—As part of upholding a fair and top-quality process, the Attribution Mechanism might include an independent internal multinational "red team/peer review" consisting of independent professionals—experts from the private and public sectors, intelligence agencies, and academia—to evaluate the process and its outcomes.

iv. Channels of Professional Communications

The International Cyber Attribution Mechanism would maintain close ties and permanent, confidential, and reliable channels of communications with any relevant entity—governmental or non-governmental—that can contribute to its efficiency and effectiveness. On one hand, it would communicate with all States parties to the Attribution Mechanism's treaty, including their relevant national intelligence and law enforcement institutions. On the other hand, it would interact with cybersecurity companies, which deal daily with detecting and investigating vulnerabilities and cyber attacks, as well as with predominant tech platforms, which also consistently detect and investigate any cyber attack conducted against or through their systems or any significant anomaly that may signify a cyber attack. The Attribution Mechanism would develop trusting relationships with these bodies that are its essential providers of relevant expertise, information, and knowledge.

v. Standard of Proof

In 2018 the Conference of States Parties of the Organization for the Prohibition of Chemical Weapons extended the Fact-Finding Mission mandate so that whenever chemical weapons are used in any State party territory, the Fact-Finding Mission should strive to identify the perpetrators "with a view to facilitating universal attribution of all chemical weapons attacks."[176] Thus, the Organization for the Prohibition of Chemical Weapons's Investigation and Identification Team that investigated the unlawful use of chemical weapons in Syria was the first to attribute responsibility to Syria, based on its findings. In doing so, the Investigation and Identification Team officially embraced a moderate standard of proof: "reasonable grounds to believe."[177] However, the statement of the team coordinator indicated that the evidence gathered in that case met the level of clear and convincing evidence. The Attribution Mechanism should also strive to meet the clear and convincing level of proof since any lower level might deliver an undesirable message of lowering the standard to make it easier to place blame, at the expense of accuracy. The Attribution Mechanism would publish its final findings and attribution determinations only if it succeeded in collecting enough evidence that met that standard of proof, and never before providing the defendant State, whether a State party or not, with the opportunity to exercise its right for a written or oral hearing within a brief period of time. A refusal to participate in such hearing procedures would not block the Attribution Mechanism from completing and publishing its final attribution determination.

vi. The Authority to Judge and Punish

Several proposals suggest authorizing international attribution institutions to assess, adjudicate, and impose punitive measures—mostly sanctions—or to

176. Press Release, OPCW, CWC Conference of the States-Parties Adopts Decision Addressing the Threat from Chemical Weapons Use (June 27, 2018), https://www.opcw.org/media-centre/news/2018/06/cwc-conference-States-Parties-adopts-decision-addressing-threat-chemical; *see also* Articles 10, 19, and 20 in the decision of the OPCW, OPCW Conference of the States-Parties, Decision Addressing the Threat from Chemical Weapons Use, C-SS-4/DEC.3 (June 27, 2018), https://www.opcw.org/sites/default/files/documents/CSP/C-SS-4/en/css4dec3_e_.doc.pdf.

177. OPCW Technical Secretariat, First Report by the OPCW Investigation and Identification Team Pursuant to Paragraph 10 of Decision C-SS-4/Dec.3 "Addressing the Threat from Chemical Weapons Use", S/1867/2020, ¶ 2.18 (Apr. 8, 2020), https://www.opcw.org/sites/default/files/documents/2020/04/s-1867-2020%28e%29.pdf.

make recommendations on reparations and sanctions. In my view, at this stage the Attribution Mechanism, like the Fact-Finding Mission and the Investigation and Identification Team mentioned above, should concentrate merely on investigating and attributing responsibility, whereas the States negotiating the establishment of the Cyber Convention should discuss and agree on an appropriate configuration for the mechanism's judicial arm. Meanwhile, an Attribution Mechanism final report would underpin the independent political decision of the victim State, whether and how to respond by virtue of international law. As for gaps in primary or secondary rules, the Attribution Mechanism should only issue recommendations. The States parties negotiating the content of the would-be Cyber Convention would take those recommendations under meticulous consideration.

vii. Implementing Advanced Technologies

Technological developments can make the attribution process faster and more accurate, to the point of detecting cyber attacks and cyber crimes even before their damage occurs. Therefore, the Attribution Mechanism must maintain close cooperation with key international entities that play a significant role in governing technological aspects of the internet. These would include the Internet Engineering Task Force, the Internet Corporation for Assigned Names and Numbers, and the International Telecommunication Union. Collaboration between these entities and the Attribution Mechanism could lead to changes in the network's architecture, enabling efficient and rapid technological detection and identification. Additionally, emerging technologies like AI could make the format of the Comprehensive Nuclear Test Ban Treaty's verification regime feasible for cyberspace with the required suitable adaptations.[178] In other words, placing hardware components at key nodes throughout the network or using AI software for permanent scanning to detect the net's anomalies may enable rapid detection and identification

178. Comprehensive Nuclear Test Ban Treaty Organization (CTBTO), *Overview of the Verification Regime*, https://www.ctbto.org/verification-regime/background/overview-of-the-verification-regime/ (last visited Aug. 15, 2024) (The monitoring system uses four complementary technologies—seismic, hydroacoustic, infrasound, and radionuclide—to detect, locate, and identify nuclear explosions anywhere on the planet. It consists of 337 facilities around the globe, monitoring the atmosphere, underground, and underwater. The system has been completely established and certified under the oversight of the CTBTO preparatory commission, however, the treaty has not yet entered into force.).

of any cyber wrongdoing. Such developments could be the crux of the Attribution Mechanism until the establishment of the Cyber Security Initiative.

Taken together, against the current decentralized attribution process, the addition of a centralized Attribution Mechanism would help engender trust in the attribution process and its findings. The structure of the Attribution Mechanism and the way it implements professional and objective methodologies, including transparent evidentiary standards and criteria that may be adapted to cyberspace, would reinforce its credibility and legitimacy. Such a mechanism is an imperative international tool to verify compliance with the List of Non-Binding Norms, while recommending how primary rules should be interpreted and applied, reinforcing deterrence, and reducing global risks.

IV. CONCLUSION

All agree that cyberspace is not the Wild West, and that it should be subject to international law. However, international cyber law is still in its infancy, and it suffers from some Wild West-like symptoms. Normative clarity and efficient law enforcement are two key interrelated factors required for ensuring the viability of international law. Neither has yet been established in the cybersphere, primarily due to the Great Power Competition. In the wake of the 9/11 terror attacks, President Bush announced a new U.S. doctrine of "zero tolerance" for terrorism.[179] However, the United States has enforced this through military capabilities, primarily against weaker States that lack political protection from major powers like Russia or China.[180] At times, American funding has also been provided to relevant States to ensure their cooperation in fighting terror. There are similarities between terrorism and cyberspace, and it is sufficient to recall that a serious destructive or disruptive cyber attack is akin to a terrorist attack. Moreover, cyber capabilities are accessible to terrorist organizations and any savvy hacker has the potential to metamorphose into a dangerous cyber terrorist in the blink of an eye. Thus, under-regulated cyberspace raises serious challenges, including global threats of cyber terrorism and cyber "Pearl Harbor" catastrophes, which the United

179. Bush, *supra* note 121, at 11 (stating that the U.S. would "ensur[e] that other states accept their responsibilities to take action against these international threats within their sovereign territory . . . . Where states are weak but willing, we will support them vigorously in their efforts. . . . Where states are unwilling, we will act decisively to counter the threat they pose and, ultimately, to compel them to cease supporting terrorism.").

180. De Nevers, *supra* note 121.

States cannot handle on its own, as President Biden has openly admitted.[181] Nonetheless, the United States remains resolute in employing its power to impose its political agenda, independently and predominantly with its closest allies in the Five Eyes, which align with this course of action. Eventually, the outcomes of the implemented policy remain poor while the risks remain high and viable. Therefore, there is a need to change the course of action. The sooner, the better.

In his speech,[182] Ambassador Mahley spoke of an out-of-the-box solution to the threat of biological weapons, unlike anything ever known before. However, since then, no formula for such a solution has ever been approved and implemented. To this day, the Biological and Toxin Weapons Convention remains without any effective mechanism to ensure States' compliance with its binding provisions. One might even claim that the COVID-19 pandemic was a direct result of this failure. We may never know whether this is true or false in the absence of findings by an independent, impartial, scientific, international investigation, which remains out of reach as long as China rejects any international call for further investigation.[183] In cyberspace, the vulnerabilities that pose enormous risks are countless and are accessible to any motivated savvy hacker who may find and covertly exploit them for criminal or politically motivated cyber attacks. A crucial approach to managing these risks—before, during, and after their occurrence—is the continuous strengthening of cybersecurity on a multinational scale. Yet this alone is insufficient. Clear and binding international regulation, accompanied by an effective enforcement mechanism, is the other side of the same coin and is crucial at the same level of urgency, or even more. In principle, this can be achieved by States—the lawmakers of international law—either proactively, primarily through binding international treaties, or relatively passively over a long period through soft law and State practice. Yet, over the past two decades, progress in both tracks has been exceedingly slow, dictated by the

181. The White House, Remarks by President Biden on America's Place in the World (Feb. 4, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/ (emphasizing that only nations "working together and in common" can solve "the accelerating global challenges"; the United States "cannot do it alone").

182. Mahley, *supra* note 1.

183. The White House, Statement by President Joe Biden on the Investigation into the Origins of COVID-19 (Aug. 27, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/27/statement-by-president-joe-biden-on-the-investigation-into-the-origins-of-covid-%E2%81%A019/.

Great Power Competition, while the disparities continue to be quite substantial and remain unsolvable through universal consensus given the tense political climate and conflicting interests. To put it bluntly, the Great Power Competition and universal consensus on significant binding international legal instruments to regulate cyberspace form an oxymoron bound to perpetuate a vicious cycle, as depicted above.

However, as this article illustrates, the United States has been implementing, along with its partners in the Five Eyes, a policy that falls far short. The number of politically motivated cyber attacks is on the rise, while the number of official and collective attributions fails to grow accordingly. Moreover, due to legitimacy deficits of the List of Non-Binding Norms, the process of collective attributions, and limited responses, the effectiveness of this policy is finite, as are its deterrent impacts on States' behavior.

Focusing on attaining a workable consensus among as many States as possible that share common moral values, rather than pursuing a formal universal consensus, would enable the international community to break this enduring vicious cycle and move forward towards a notable change aimed at establishing the "Triple -I," an international and more legitimate three-tiered legal regime for cyberspace. As elaborated in this article, the first "I" to be established is a tier focused on establishing a centralized, independent, and impartial International Cyber Attribution Mechanism that would function with close cooperation by all its States parties and with any pertinent reliable entity from the private sector, civil society, and academia. The Attribution Mechanism's purpose is to serve as an authorized international mechanism for investigating politically motivated cyber attacks according to transparent criteria and guidelines. Once the findings allow, the Attribution Mechanism would produce official attribution determinations. As explained, such attributions would be immeasurably more credible and legitimate than the current national attributions.

Subsequently, the workable consensus would be extended to include the next "I," the International Cyber Security Initiative. This would be built on top of the List of Non-Binding Norms and other relevant international conventions to serve as a global security regime or an international cyber security arm to enhance States' capabilities, accountability, and deterrence The International Counter Ransomware Initiative could serve as a significant foundation for such a global and centralized body, and both could even be merged.

Thereafter, the workable consensus should be enhanced by including the third "I"—the International Cyber Law Convention. This is a comprehen-

sive treaty that would clearly articulate which rules and legal norms are binding in cyberspace and how they should be applied. The Cyber Convention must fully correspond with the Attribution Mechanism and Cyber Security Initiative and vice versa. In fact, the Attribution Mechanism and Cyber Security Initiative might be incorporated into the Cyber Convention as its exclusive mechanisms for investigation, attribution, and enforcement.[184]

The United States is the most vulnerable State in cyberspace, while at the same time being the most influential architect in the under-regulated cyberspace. However, American arguments against the establishment of an international cyber law treaty are not convincing. They seek to perpetuate a situation in which the United States uses its power to impose rules of conduct whose exact content the United States determines retroactively and according to its own interests.

A year ago, the U.S. Secretary of State explained how crucial it is for the United States to sit at the negotiating table and help shape the rules and standards by which technology is used in ways that reflect U.S. interests and values, not those of China or Russia.[185] This is at the same time as China and Russia have been endeavoring to achieve the opposite. As a result, the adoption and implementation of the Triple I, even incrementally or partially, but at least moving forward in a similar direction based on a workable consensus, hinges primarily on American political will and perseverance, which, as expressed by the Secretary of State, are quite distant.

If the United States truly accepts the proposed approach, American political perseverance will ensure that any obstacle or problem arising during the negotiations could be resolved. Furthermore, while the proposed regime is not immune to residual risks, including the risk of exposing classified intelligence and capabilities or being constrained by rules that rival powers might not uphold, these risks are manageable. The benefits would far outweigh the risks associated with maintaining the current level of under-regulation in cyberspace and the existing vicious cycle.

In sum, the United States is the most influential power among dozens of States that share common values. These common values should be safeguarded in cyberspace through a new legal regime. Where there is a will there

184. As explained above, while it is theoretically possible to establish both together in one convention, given the ambitious nature of this goal, it may be more reasonable to pursue them in separate stages.

185. Antony J. Blinken, Sec'y of State, Remarks to the Press at Stanford University (Oct. 17, 2022), https://www.state.gov/secretary-antony-blinken-remarks-to-the-press-3/.

is a feasible way to build a workable consensus and realize the Triple I regime. Sweeping opposing arguments, even those related to important national security interests, should not be accepted outright; they can and should be carefully balanced.