PROMOTING INTERNATIONAL CYBERSECURITY COOPERATION: LESSONS FROM THE PROLIFERATION SECURITY INITIATIVE

Duncan B. Hollis & Matthew C. Waxman***

ABSTRACT

Global efforts by states to cooperate through international rules in combating cyber threats have generated mixed results, at best. In this paper, we examine the architecture of the Proliferation Security Initiative (PSI) as a possible model for future cybersecurity cooperation among interested states. We identify several features of PSI's architecture (rather than its substantive focus on non-proliferation) for further analysis, including PSI's low entry costs, tiered structure, and flexibility, as well as its leveraging of both territorial jurisdiction and state consent. We conclude that, despite several hurdles visible in the scope of its membership and its legal framework, PSI still offers worthwhile parallels to draw upon, suggesting a new framework that could allow interested states to further cooperate in addressing current cyber threats.

TABLE OF CONTENTS

I. INTRODUCTION

Cybersecurity threats have become ubiquitous. Today, cyber-attacks by state and non-state actors—including disruption of infrastructure, large-scale theft of data and intellectual property, hacking of political actors and election systems—are generating significant losses. These losses, moreover, are occurring across a range of metrics, including national security, privacy, and economics.

Global efforts by states to cooperate through international rules in combatting these threats have generated mixed results, at best. For example, in 2013, a United Nations Group of Governmental Experts (U.N. GGE), including experts from the Chinese, Russian, and U.S. governments, adopted a consensus report indicating that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [(information and communication technology)]

environment."[1] This view was confirmed by another U.N. GGE in 2015, which also endorsed a series of voluntary (i.e., non-legally binding) norms for responsible state behavior.[2] These included prohibiting states from peacetime targeting of critical infrastructure and the work of computer security incident response teams (CSIRTs).[3] Unfortunately, much of the GGE's momentum was lost in 2017 when the latest GGE failed to generate any report. According to the U.S. expert at the negotiations,

> [d]espite years of discussion and study, some participants . . . seem to want to walk back progress made in previous GGE reports. I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions.[4]

With the recent GGE's failure, attention has shifted to other fora for cultivating international cybersecurity rules. Some efforts—like the non-governmental Global Commission on the Stability of Cyberspace—are focused on reaching new universal

---

The genesis for the essays that comprise issue 32.2 of this Journal was a May 2017 workshop hosted at Temple University, and co-hosted with Leiden University. Under the theme "Influencing International Behavior in Cyberspace: Devising a Playbook of Consequences for Cyber Incidents," the workshop gathered a broad array of academic and governmental experts. Participants included representatives of the Estonian, Finnish, and U.S. governments (including officials from the Department of Defense, the State Department, and the U.S. Trade Representative). All government officials, however, participated in their personal capacity. As such, the views expressed in this special issue should not be attributed to any government or government agency.

* Professor of Law and Associate Dean for Academic Affairs, Temple University Beasley School of Law; Non-Resident Scholar, the Carnegie Endowment for International Peace.

** Liviu Librescu Professor of Law, Columbia Law School; Co-Chair, Cybersecurity Center, Columbia Data Science Institute; Adjunct Senior Fellow, Council on Foreign Relations.

1. *See* U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter *2013 GGE Report*]. The GGE process is, of course, not the only vehicle for inter-state cooperation on cybersecurity. In 2015, for example, President Barack Obama and President Xi Jinping announced a "common understanding" on cyberespionage. They agreed that neither the U.S. nor the Chinese government "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." *See* OFFICE OF PRESS SEC'Y, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT TO THE UNITED STATES (2015). This principle was later endorsed by the G-20. *See* G-20 Leaders' Communiqué, *Antalya Summit*, (Nov. 15–16, 2015), ¶ 26, http://www.mofa.go.jp/files/000111117.pdf. The Trump administration and the Xi Government also recently reaffirmed the prohibition on cyber-espionage. Cory Bennett, *Why Trump is Sticking with Obama's China Hacking Deal*, POLITICO (Nov. 8, 2017, 5:29 AM), https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658.

2. U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 10, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter *2015 GGE Report*].

3. *See id.*, ¶ 13(h), (k).

4. Michele Markoff, U.S. Expert to the Group of Governmental Experts, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security* (June 23, 2017), https://usun.state.gov/remarks/7880.

agreements on substantive standards for state behavior.[5] Meanwhile, Microsoft President and Chief Legal Officer Brad Smith has been promoting a "Digital Geneva Convention," which notably includes a call for global technology companies to agree to a set of rules on cybersecurity.[6]

Cooperation in cybersecurity, however, need not always involve devising new norms, rules, interpretations or principles any more than it must involve all states.[7] Progress can come through the development of new processes among like-minded groups of states and other stakeholders that seek to effectuate existing international laws and other norms.

In this vein, the Proliferation Security Initiative (PSI) is often cited as a possible model for future cybersecurity cooperation.[8] Some have already analyzed whether the PSI's approach to the interdiction of weapons of mass destruction (WMD) could apply to cybersecurity.[9] In this essay, we offer a different analysis, examining the architecture of PSI's cooperative mechanisms (rather than its contents) as a possible model for future cybersecurity cooperation among interested states. We conclude that there are worthwhile parallels to draw upon, which could allow interested states to further cooperate in addressing current cyber threats.

II. THE PROLIFERATION SECURITY INITIATIVE

In December 2002, a North Korean freighter, the *So San*, was transiting the Arabian Sea without flying a flag and with a newly painted hull that obscured its name and home port. U.S. intelligence officials asked Spanish marines to board and

5. *See, e.g.*, *Global Commission Proposes Call to Protect the Public Core of the Internet*, GLOB. COMM'N ON THE STABILITY OF CYBERSPACE (Nov. 21, 2017), https://cyberstability.org/news/global-commission-proposes-action-to-increase-cyberspace-stability/ (describing the GCSC Commissioners declaration urging state and non-state actors to avoid activity that would intentionally and substantially damage the general availability or integrity of the "public core" of the internet). For details on the composition and mission of the GCSC, see GLOB. COMM'N ON THE STABILITY OF CYBERSPACE, https://cyberstability.org (last visited Feb. 17, 2018).

6. Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT BLOG (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. In the interest of full disclosure, one of us—Duncan Hollis—is presently advising Microsoft on international legal issues relating to its proposal.

7. *See, e.g.*, Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 427, 465 (2016).

8. See, e.g., Testimony of Christopher Painter, Coordinator for Cyber Issues, U.S. Department of State, *Cybersecurity: Setting the Rules for Responsible State Behavior*, SUBCOMMITTEE OF EAST ASIA, THE PACIFIC AND INTERNATIONAL CYBERSECURITY POLICY, SENATE FOREIGN RELATIONS COMMITTEE, S. HRG. 114-76, May 14, 2015, 21; Joseph Marks, *Report: DoD needs to improve cybersecurity, resilience – Cyber ripe for cooperation, GOP leaders say*, POLITICO, Jan. 22, 2015, https://www.politico.com/tipsheets/morning-cybersecurity/2015/01/report-dod-needs-to-improve-cybersecurity-resilience-cyber-ripe-for-cooperation-gop-leaders-say-212543.

9. *See, e.g.*, Trey Herr, *Governing Proliferation in Cybersecurity*, 3 GLOB. SUMMITRY 1 (2017).

search the ship as a "stateless" vessel.[10] On board, they discovered fifteen Scud missiles hidden under bags of cement. Efforts to seize these missiles, however, were unavailing.[11] The Yemeni government informed U.S. and Spanish authorities that they had purchased the missiles, and, in the absence of international law rules against transporting such materials, those authorities allowed the delivery to proceed.[12] The event was seen as evidence of both (i) how seriously many states take the international law principle that "vessels on the high seas are subject to no authority except that of the state whose flag they fly"[13] and (ii) serious gaps in states' collective capability to deal with the proliferation of weapons of mass destruction, their delivery systems, and related goods.[14]

Within a year, the United States and Spain were among eleven founding members of the PSI, a joint effort to strengthen the "political commitment, practical capacities, and legal authorities necessary to stop, search, and, if necessary, seize vessels and aircraft believed to be transporting 'weapons of mass destruction, their delivery systems, and related materials.'"[15] PSI was not, however, a typical treaty-based international institution. Rather, it came into existence by virtue of states endorsing a political commitment, the *Statement of Interdiction Principles* (SIP).[16]

A short document, the SIP identifies the proliferation of WMD as a common threat, and pledges endorsing states to four sets of activities:

1. To "undertake effective measures" to interdict "the transfer or transport of WMD, their delivery systems, and related materials to and from states and

10. *See* United Nations Convention on the Law of the Sea, art. 110, Dec. 10, 1982, 1833 U.N.T.S. 397 (authorizing a warship to board a foreign ship that appears to be without nationality). When Spanish authorities tried to board the *So San*, its master claimed the vessel was Cambodian, leading to a request to Cambodia that Spanish forces be allowed to board the vessel—permission that Cambodia granted. *See* U.S. DEP'T OF STATE, BRIEFING, PROLIFERATION SECURITY INITIATIVE, FED NEWS SERVICE 12 (2003).

11. *See* Michael Byers, *Policing the High Seas: The Proliferation Security Initiative*, 98 AM. J. INT'L L. 526, 526 (2004).

12. *See* Joel A. Doolin, *The Proliferation Security Initiative: Cornerstone of a New International Norm*, 59 NAVAL WAR C. REV. 29, 30 (2005) (describing how international laws enabled *So San* to transport Scud missiles); *see also* Byers, *supra* note 11, at 526; Thom Shanker, *Threats and Responses: Arms Smuggling; Scud Missiles Found on Ship of North Korea*, N.Y. TIMES (Dec. 11, 2002), http://www.nytimes.com/2002/12/11/world/threats-and-responses-arms-smuggling-scud-missiles-found-on-ship-of-north-korea.html.

13. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, ¶ 64 (Sept. 7).

14. *See* Byers, *supra* note 11, at 527 ("Traffickers can take advantage of flags of convenience—registering their vessels in states that provide little in the way of regulation and oversight—or use vessels flagged by states that steadfastly refuse to consent to the exercise of high seas jurisdiction by others.").

15. *Id.* at 528. Before the Statement of Interdiction Principles (SIP), the PSI idea was first announced in a presidential press conference in Poland. *See* President George W. Bush, Former President of the U.S., Remarks by the President to the People of Poland at Wawel Royal Castle in Krakow (May 31, 2003), *available at* https://georgewbush-whitehouse.archives.gov/news/releases/2003/05/20030531-3.html.

16. *See* AARON DUNNE, THE PROLIFERATION SECURITY INITIATIVE: LEGAL CONSIDERATIONS AND OPERATIONAL REALITIES SIPRI PAPER NO. 36 vii (Stockholm Int'l Peace Res. Inst., 2013) (noting that the aims of PSI were to limit the delivery and transport of WMD).

non-state actors of proliferation concern;"[17]

2. To streamline procedures for "rapid exchange of relevant information concerning suspected proliferation activity," including protecting the confidentiality of shared information and dedicating "appropriate resources and efforts to interdiction operations and capabilities;"[18]
3. To strengthen "relevant national legal authorities" and "relevant international law and frameworks" to accomplish the PSI's objectives;[19] and
4. To prevent the transport of covered materials where there is a reasonable suspicion that a vessel or aircraft is carrying them, including boarding and searching vessels flying the endorsing state's flag (or consenting to other states doing so); requiring aircraft to land for inspection; and inspecting vessels at transshipment points within its jurisdiction; and seizing covered goods.[20]

The SIP directs that all PSI activities should occur only to the extent consistent with an endorsing state's national laws and its obligations under international law.[21]

Other states were invited to join the PSI, and as of today, 105 states have endorsed the SIP.[22] Participation is subdivided between a core group of twenty-one states comprising the "Operational Experts Group" which has the greatest capacity to undertake counter-proliferation activities, and other endorsing states.[23] For those states looking to build capacity, the PSI has produced a Model National Response Plan.[24]

At its core, PSI references a set of activities rather than establishing an institution.[25] To date, it is credited with dozens of interdictions of WMD-related

17. U.S. DEP'T OF STATE, PROLIFERATION SECURITY INITIATIVE: STATEMENT OF INTERDICTION PRINCIPLES, at princ. 1 (2003), https://www.state.gov/t/isn/c27726.htm (defining "[s]tates or non-state actors of proliferation concern" as those involved in "(1) efforts to develop or acquire chemical, biological, or nuclear weapons and associated delivery systems; or (2) transfers (either selling, receiving, or facilitating) of WMD, their delivery systems, or related materials").

18. *Id.* at princ. 2.

19. *Id.* at princ. 3.

20. *Id.* at princ. 4 (offering an illustrative list of six activities participating states could take in "support of interdiction efforts regarding cargoes of WMD, their delivery systems, or related materials to the extent their national legal authorities permit and consistent with their obligations under international law and frameworks . . .").

21. *Id.* at pmbl., princ. 4.

22. *PSI Endorsing States*, PROLIFERATION SECURITY INITIATIVE, http://www.psi-online.info/Vertretung/psi/en/03-endorsing-states/0-PSI-endorsing-states.html (last visited Apr. 12, 2018). A good discussion of this wide invitation can be found in SUSAN J. KOCH, OCCASIONAL PAPER 9: PROLIFERATION SECURITY INITIATIVE: ORIGINS AND EVOLUTION 19–20 (2012), http://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Occasional%20Papers/09_Proliferation%20Security%20Initiative.pdf.

23. DUNNE, *supra* note 16, at vii, 6. The Operational Experts Group is further divided into specific regional groupings. *Id.* at 6.

24. *Id.* at 5.

25. *Id.* at 43.

materials.[26] This success comes even as—or perhaps because—the PSI is loosely organized. It pushes states to develop and exercise jointly the necessary domestic legal tools to deal with WMD proliferation. But it also leaves states to decide for themselves who are "states and non-state actors of proliferation concern"[27] and what constitutes "reasonable suspicion."[28] This gives participating states considerable latitude to interpret what behavior conforms to PSI and whether to label an interdiction as PSI-related.[29]

Originally, PSI was controversial because of perceptions that its participants were seeking to change the international legal rules relating to the freedom of the high seas.[30] In practice, however, most PSI activities occur *within* a participating state's territory or with the permission of the flag state or the aircraft's state of registration.[31] In other words, PSI's primary impacts have occurred within domestic legal frameworks wherein states deploy their own resources (or consent to others doing so) in ways consistent with the SIP's broadly stated goals. The result is a system of cooperation that is not so much collective as it is coordinated.

That said, the PSI has not ignored international law entirely. Bilaterally, the United States has entered into at least eleven "ship-boarding" treaties where the parties give advance consent to the other sides' search of any of its flagged vessels suspected of WMD trafficking, thereby paving the way for PSI operations.[32] PSI participants have also called for more widespread participation in the Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) and greater implementation of various U.N. Security Council Resolutions on WMD proliferation (particularly those relating to North Korea and Iran).[33] In that regard, PSI has helped make existing international law work more effectively. At the same time, participants have not sought to modify the

26. Emma Belcher, COUNCIL ON FOREIGN REL., *The Proliferation Security Initiative: Lessons for Using Nonbinding Agreements* 1 (2011), https://www.cfr.org/content/publications/attachments/IIGG_WorkingPaper6_PSI.pdf; *see also* Herr, *supra* note 9, at 16 (describing PSI as "moderately successful").

27. STATEMENT OF INTERDICTION PRINCIPLES, *supra* note 17, at princ. 1.

28. *Id.* at pmbl. (The source text uses "reasonably suspected" when discussing what we have termed as "reasonable suspicion" here.)

29. *See* DUNNE, *supra* note 16, at 10 (noting the lack of formal methods for determining whether certain activities constitute a PSI interdiction).

30. *See generally* Daniel H. Joyner, *The Proliferation Security Initiative: Nonproliferation, Counterproliferation, and International Law*, 30 YALE J. INT'L L. 507 (2005).

31. *See* DUNNE, *supra* note 16, at 35 (noting that, despite the *So San* incident serving as the PSI catalyst, interdictions in international waters are "extremely rare").

32. *See, e.g.*, Agreement between the Government of the United States of America and the Government of the Republic of Cyprus Concerning Cooperation to Suppress the Proliferation of Weapons of Mass Destruction, Their Delivery Systems, and Related Materials By Sea, Cyprus-U.S., July 25, 2005, Department of State Press Releases, https://www.state.gov/t/isn/trty/50274.htm.

33. *See, e.g.*, Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, IMO Doc. LEG/CONF.15/21 (Nov. 1, 2015); Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 221; S.C. Res. 1737 (Dec. 23, 2006) (concerning Iran's nuclear weapons program and non-cooperation with prior U.N. resolutions); S.C. Res. 1540, ¶ 3 (Apr. 24, 2004) (requiring all states to "establish domestic controls to prevent" WMD proliferation).

basic international maritime law framework.

In sum, the PSI offers an innovative approach to cooperation by a "coalition of the willing" against a global threat via loose coordination of national and international toolsets. As such, it might serve as a model for addressing issues of global cybersecurity.[34] We believe that there are good reasons for the comparison. Specifically, there are several key aspects of the PSI that appear well-suited to one or more cybersecurity problems.

III. POSITIVE PROLIFERATION SECURITY INITIATIVE FEATURES FOR GLOBAL CYBERSECURITY

Ultimately, the real value of PSI as a possible model for global cybersecurity lies not in the specific activities that it asks participating states to endorse, but the institutional architecture by which it does so.[35] In other words, we are not arguing for a policy of more aggressive interdiction or counter-proliferation of dangerous cyber tools; rather, we are looking to WMD interdiction for lessons on cultivating international cooperation for a gamut of cybersecurity challenges. For example, as states seek to build consensus around appropriate responses to unlawful cyber behavior—or behavior in violation of norms promoted by bodies like the U.N. GGE—a PSI architecture provides a potentially novel way to encourage collective action without necessitating legally binding commitments or changes to extant laws and norms.

We briefly summarize below eight ways in which a PSI-like approach might be attractive to states for addressing some cybersecurity issues: (i) orientation, (ii) low entry costs, (iii) tiered structure, (iv) leveraging territorial jurisdiction, (v) leveraging state consent, (vi) flexibility, (vii) processes of evolution, and (viii) experimentation. At the same time, we also note two challenges that need attention before pursuing a PSI framework for dealing with cyber threats: issues of hegemony and differing background legal frameworks. On balance, we conclude that the PSI architecture offers a potential model for coordinating international cooperation, not to halt trade in malicious cyber tools, but rather to coordinate state responses to unwanted cyber behavior.

A. Potential Benefits of a PSI Approach

As a model for promoting international cooperation and developing stronger international rules for cybersecurity, PSI has many attractive or instructive features, including the following.

---

34. *See* Herr, *supra* note 9, at 5 ("Developed to interdict the spread of WMD devices, as noted above, the PSI has occupied a central role in the discussion over proper analogies for cybersecurity and proliferation, most prominently through informal proposals by some in the U.S. State Department.").

35. Thus, we should not be read to endorse an exclusively "proliferation" focused model for dealing with cybersecurity. Nor do we mean to suggest that cybersecurity itself is a single problem set that warrants a unitary solution; it involves a diverse set of problems such that we believe one or more of them might benefit from a framework modeled off the PSI experiences to date.

1. Orientation

PSI endorsing States share a common cause in combating WMD participation and view PSI as complementary to other existing responses. A PSI-like approach to cybersecurity could adopt a similar framework, using the affiliation to delineate commonly held norms among a group of like-minded states and offering the framework as complementing—rather than competing with—other existing responses.

2. Low Entry Costs

As a coalition of the willing, PSI assumes cooperation can begin with a political commitment by just a few states. A similar commitment for cybersecurity would also not require onerous domestic approval processes associated with formal international legal institutions or instruments. And by framing the scope of activities to accord with extant domestic and international legal authorities and capacities, such a framework would take states as it finds them. At a time when global coalitions face division and dissension, there may be some appeal for allowing a like-minded group of states to set out a coordination framework against one or more types of cyber threats.

3. Tiered Structure

The PSI accepted that some states have the resources and tactical skills to deal with proliferation while others did not, adopting a framework to accommodate this disparate capacity. One could envision a similar division in cybersecurity where some states have a much greater capacity to identify and respond to cybersecurity threats on which others may depend, with assurances that doing so would not violate national or international legal regimes.

4. Leveraging Territorial Jurisdiction

One of the PSI's great strengths is recognizing how much extant international maritime law defers to national authorities and the exercise of a state's jurisdiction within its territory, ports, and internal waters. If states build up their domestic capacities to counter cyber threats, the PSI experience suggests that there can be systemic benefits. Leaving states to act autonomously but according to a collective framework may leave some relatively ungoverned spaces, but if national behaviors reflect a sufficiently uniform and general practice it could substantially restrict the ability of hostile actors to operate effectively. And while there was a time when many questioned the ability of territorial jurisdiction to operate vis-à-vis cyberspace, in recent years many states have demonstrated strong interest and sufficient capacity to regulate cybersecurity on territorial grounds.[36] Thus, the first line of defense for responding to global cyber threats may lie in coordinating better domestic authorities and responsive operations.

36. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006).

5. Leveraging State Consent

With few exceptions, international law defers to state consent to delimit lawful from unlawful behavior.[37] Thus, where a state consents to another PSI participating state's activities on its vessels or in its territorial seas, there are far fewer legal issues than where such consent is absent. Likewise, cybersecurity might benefit from a similar push for a state's consent (whether formalized in advance or on an ad hoc basis) to other participating state's defensive operations in its networks or systems. This would take the coordination contemplated by the Budapest Convention on Cybercrime[38] and elevate it to an even more integrated response. We might imagine, for example, some number of states agreeing that one state could conduct network investigative techniques against actors who are the source of cyber threats and operating in the territory of another participating state.

6. Flexibility in Defining and Enforcing Norms

The PSI has allowed states to align around a core suite of activities while acknowledging and accommodating different national approaches, as well as different interpretations of international law (or desires for the evolution of international law to accommodate proliferation-related restrictions on freedom of navigation on the high seas).[39] Although these ambiguities have led some to criticize PSI as being too malleable, this flexibility in coordinating around general norms rather than precise ones may be attractive to states suspicious or wary of being locked in to specific actions (or inactions). A PSI approach could take existing norms (e.g., not targeting critical infrastructure in peacetime, not using CSIRTs for malicious purposes) and leave to individual participants the precise contours by which they understand what the norms mean. Further precision could come over time as parties respond to different sorts of behavior, although there is a risk that the iterations might go the other way and lead to a norm's failure.[40]

7. Process of Evolution

The PSI is a "voluntary" affiliation that was able to take advantage of the participation of key actors and grow from less than a dozen states to more than one hundred today. A similar strategy could be employed in developing a schedule of consequences for unwanted cyber behavior. As PSI shows, there is no need to obtain the consent of all the major players at once; but rather, a few key gatekeepers can start the process, even in the face of significant opposition. (It is worth recalling that a number of states, such as India and China, have publicly opposed PSI.) A major design question from the outset is how easy or hard it would be to make such an

37. States cannot, however, consent to *jus cogens* violations such as genocide, unlawful use of force, or torture.

38. Council of Europe, *Convention on Cybercrime*, COUNCIL OF EUROPE (Nov. 23, 2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

39. *See* KOCH, supra note 22, at 13, 26–27 (discussing diplomatic and collaborative efforts made by PSI states).

40. *See* Finnemore & Hollis, *supra* note 7, at 467 (noting that with respect to norm promotion efforts, "[f]ailure remains an option (and may even be the dominant outcome)").

initiative to join, balancing wider participation with less precise or onerous expectations of cooperation or consent.

8. Experimentation

Understanding that a PSI-like cybersecurity experiment could evolve over time leaves room for the participating states to experiment with different shared activities. In the PSI context, for example, states' initial focus on international maritime interdiction gave way to more productive—and more easily legitimated—port-state efforts to deal with the transport and trans-shipment of WMD-related materials. A similar dynamic approach in cybersecurity could accommodate the reality that some efforts may fail and others may emerge where cooperation might be most productive.

B. Challenges in Applying PSI

In endorsing further analysis of the PSI model for cybersecurity, we are aware that the analogy is not perfect. The PSI also has at least two problematic features that may limit its effectiveness in promoting cybersecurity cooperation: (i) representation; and (ii) varying legal frameworks.

1. Hegemonic and Underrepresented

PSI has been criticized for being a tool of U.S. hegemony with key parts of the world (e.g., the Middle East and Africa) under-represented, despite those very areas being at the highest risk for WMD proliferation. A U.S.-led effort in cybersecurity could face similar charges. Indeed, there is the possibility that if the United States and a like-minded coalition pursued a PSI-like framework for cybersecurity, a competing coalition might be formed by "internet sovereignty" states such as China. The result would be two or more rival coalitions looking to actively undermine each other.

2. Different Background Legal Frameworks

Despite U.S. frustration with Yemen getting its Scud missiles in the *So San* incident, there was remarkable unanimity about both the underlying unlawfulness of proliferation *and* what interdictions international law allows and those it prohibits (i.e., those of a vessel on the high seas without its flag state's consent).[41] That certainty gave the PSI room to work around the law's limitations (e.g., by negotiating ship-boarding agreements), and to focus on non-controversial interdictions (i.e., by a port state, the flag state, or with the permission of a flag state or the state of an aircraft's registration). For cyberspace, however, *how* international law applies is currently much less clear. Efforts like the Tallinn Manual (both the original and 2.0 versions) may be celebrated for highlighting the extent to which

41. *See, e.g.*, DUNNE, *supra* note 166, at 26–27 (noting how implementation of the 1968 Nuclear Non-Proliferation Treaty (NPT), the 1972 Biological and Toxin Weapons Convention (BTWC), and the 1993 Chemical Weapons Convention (CWC) "provide much of the national legal basis required for undertaking the actions contained within the SIP" because they "ban or control the possession (with some exceptions) and trade in WMD, their means of delivery and dual-use goods").

various international law prohibitions and requirements apply in cyberspace.[42] Yet, a close reading of the text of both editions evidences extensive and substantial interpretative disagreements even among its Independent Group of Expert authors (e.g., on defining an armed attack under the *jus ad bellum*).[43] Moreover, outside the Tallinn process, others have questioned the very existence in cyberspace of some of the international law rules identified in the Tallinn Manual (e.g., self-defense, sovereignty, due diligence).[44] In such circumstances, where there is little agreement on the boundaries of permissible or impermissible behavior, it necessarily complicates efforts to respond to conduct which some group of states considers wrongful. Other states may contest not only the consequences brought to bear, but also the idea that the original behavior even deserved a sanction in the first place.

IV. CONCLUSION: A PROMISING MODEL

On balance, PSI offers a governance model that could be fruitful in addressing cybersecurity issues in the current environment. Like proliferation issues, cybersecurity cooperation could benefit from an orientation that accepts the reality of persistent threats and seeks to mitigate or remediate them. With the failure of the 2017 U.N. GGE, moreover, prospects for further universal, global efforts appear to be on hiatus. As such, plurilateral projects are currently a more viable alternative for cooperation. Like-minded states could, for example, coalesce cooperation around the enforcement of specific, agreed-upon norms of behavior, such as those articulated by the U.N. GGE in 2015 (e.g., protecting critical infrastructure from malicious cyber threats, assisting others whose critical infrastructure is threatened, sharing information, responsibly reporting vulnerabilities, and assisting the victims of the most severe cyber threats).[45] State capacity to conform to these norms is, of course, highly varied. But, that is precisely where a PSI-like tiered structure could prove useful as those with capacity take action, including with the consent of other

42. MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (NATO CCD COE, 2017) [hereinafter TALLINN 2.0]; MICHAEL N. SCHMITT (ED.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (NATO CCD COE, 2013). Although funded by NATO's Cyber Defense Centre of Excellence, both manuals represent the work of an independent group of experts.

43. TALLINN 2.0, *supra* note 2, at 341 ("[T]he law is unclear as to the precise point at which the effects of a cyber operation qualify that operation as an armed attack.").

44. States like China and Cuba resist the idea that armed attacks can occur in cyberspace sufficient to trigger the right of self-defense. JULIAN KU, HOW CHINA'S VIEWS ON THE LAW JUS AD BELLUM WILL SHAPE ITS LEGAL APPROACH TO CYBERWAREFARE, AEGIS PAPER NO. 1701, at 2 (2017), https://www.hoover.org/sites/default/files/research/docs/ku_webreadypdf.pdf; Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, LAWFARE (July 14, 2017, 1:51 PM), https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well; *see also* Colonel Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ (Writing in a personal capacity, the current legal adviser to U.S. Cyber Command questions whether sovereignty is clearly a rule of international law as opposed to a background principle that informs the meaning of other rules (e.g., non-intervention), while also noting that "[l]ike sovereignty, the applicability and scope of the due diligence rule to cyberspace is hardly a settled issue.").

45. *2015 GGE Report*, *supra* note 2, ¶13.

participating states where necessary. Focusing operations within participating state territories and employing consent to such operations could, moreover, go a long way to ensuring a project, like PSI, works within the bounds of existing national and international legal authorities.

Ultimately, a PSI-like model for cybersecurity recognizes that the current dynamic environment requires flexibility with the idea that the most effective measures can evolve, over time, into best practices for global cybersecurity cooperation. For now, it is enough to suggest that a like-minded, voluntary group of states acting autonomously but cooperatively could improve on the status quo. In the critical infrastructure context, for example, a PSI-like model could avoid the problem of defining what constitutes "critical infrastructure," focusing instead on identifying a set of common practices (e.g., information sharing, capacity building, mutual legal assistance, domestic law enforcement actions, etc.) designed to protect whatever infrastructure each state views as critical.

Our point is not, however, to argue for or against particular cooperative mechanisms. Our aim is more modest—to emphasize how the architecture in which any cybersecurity cooperation efforts rest matters. And to the extent there are obvious roadblocks, it makes sense for any PSI-like model to accommodate these rather than run into them. For example, to avoid charges of hegemony, cybersecurity cooperation should take advantage of distributed capacities to ensure that those with the capacity provide technical assistance and other capacity-building measures (e.g., information sharing or technical training) to encourage participation by less capable states. Such exchanges would not, however, be necessarily one-sided. States with less capacity can still add their voice to operations by the more skilled subset of participating states, whether to endorse efforts to halt or take down sources of malicious cyber activity elsewhere or to consent to doing so in their own territories. The broader the coalition standing behind the actions of capable states, the greater the potential impact is upon other states weighing whether to engage in malicious behavior.

Similarly, differences over *how* international laws apply to cyberspace caution against building a PSI-like model for cybersecurity that focuses on enforcing such laws, at least until such time when states agree more precisely on what the law is or what it means. Instead, cooperation could focus on improving cybersecurity by coordinating around national legal authorities within participating state territories. Certainly, such an approach would not do much to deal with safe havens in non-participating states, just as PSI leaves open possibilities of proliferation in non-participating territories. Yet, by seeking to silo off particular areas and coordinate acceptable bounds of behavior within those areas, cybersecurity conditions may improve even with the continued risk of threats from outside participating state territories.

The time is ripe for new approaches to cybersecurity cooperation. We believe the PSI deserves further consideration as a candidate for the architecture of such activities. And we say "a" candidate deliberately. We should not be interpreted to suggest that a PSI-like approach is the only—or even the best—solution going forward. The economic, privacy, and national-security implications of the manifold suite of cyber threats counsel for a multi-pronged response. Still, we believe that the PSI should be considered as one of several processes that can help restore trust in

the ICT environment and ensure a future where cyberspace is more open, stable, and secure.