BEYOND NORMS: USING INTERNATIONAL ECONOMIC TOOLS TO DETER MALICIOUS STATE-SPONSORED CYBER ACTIVITIES

*Kathleen Claussen**

ABSTRACT

In thinking about strategy and doctrine for cyberspace, one cannot ignore either the cyber domain's interaction with other domains or the applicability of existing legal tools to address cyberspace issues. This Comment focuses on the latter and argues that any discussion regarding deterrence and a playbook for consequences for cyber incidents by state actors ought necessarily to include a careful examination of existing plays, particularly where those incidents have an economic component as many do. Focusing on multilateral institutions, regional and bilateral trade and investment agreements, and unilateral tariff and non-tariff trade and investment tools, this Comment maintains that current and available international economic tools offer significant potential to shape cyber activities and norms and only now are beginning to be deployed this way.

TABLE OF CONTENTS

I. INTRODUCTION

The September 2015 joint statement by Chinese President Xi Jinping and U.S. President Barack Obama declared that each state would refrain from certain malicious cyber activities[1] was heralded by some as a meaningful commitment to

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.

evolving norms regarding appropriate state behavior in cyberspace.[2] Shortly thereafter, other countries made similar announcements jointly with China.[3] Commentators remarked on the significance of these announcements suggesting a change in China's attitude toward malicious cyber activity, even amid some warranted skepticism.[4] These announcements, while important to the reaffirmation of norms[5] and the long-term development of customary international law, are not enforceable by states or private persons.[6] Where a state finds another state acting inconsistently with their jointly affirmed norms, the aggrieved state may choose to undertake actions to signal its disagreement, but its legal options for recourse are limited.

Across national boundaries, scholars and policymakers likewise seek to enhance these nascent norms that cover many different types of malicious cyber activities.[7] The problem underlying the need for such norms is clear. For years,

---

* Associate Professor, University of Miami School of Law. Thanks to Duncan Hollis and Eneken Tikk for providing an opportunity to exchange views on this important issue. Thanks also to Gary Brown, Jeffrey Dunoff, Harvey Rishikof, and the other participants in the symposium for their thoughtful comments, and to the members of the staff of the *Journal* for their helpful edits. These comments do not reflect the views of the organization with which I have been or am affiliated.

1. *See* THE WHITE HOUSE, *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference* (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint (detailing the cyber-security agreement between the United States and China).

2. *See* David Jackson, *Obama, Xi Vow Cooperation on Climate, Cyber Issues*, USA TODAY (Sept. 25, 2015), https://www.usatoday.com/story/news/world/2015/09/25/obama-xi-jinping-china-state-visit-cybersecurity-white-house/72789436/ (describing various responses to news of the agreement).

3. *See, e.g.*, Thomas Escritt & Michelle Martin, *Ahead of Fractious G20, Germany and China Pledge New Cooperation*, REUTERS (July 5, 2017), https://www.reuters.com/article/us-g20-germany-china/ahead-of-fractious-g20-germany-and-china-pledge-new-cooperation-idUSKBN19Q16R (describing an agreement between China and Germany); Rowena Mason, *Xi Jinping State Visit: UK and China Sign Cybersecurity Pact*, GUARDIAN (Oct. 21, 2015), https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron (highlighting a new cyber-security agreement between China and the United Kingdom).

4. *See* Jackson, *supra* note 2 (presenting both praise and skepticism about the agreement, including indications from the United States of plans to work with smaller groups of like-minded partners to develop and shape cyber norms).

5. *See* Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425 (2016) (analyzing common themes between cyberspace norms); Samuel J. Rascoff, *The Norm Against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections*, 83 U. CHI. L. REV. 249 (2016) (explaining the norm against economic espionage); Mei Gechlik, *Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses*, HOOVER INST. WORKING GRP. ON NAT'L SEC., TECH., & L., AEGIS SERIES PAPER NO. 1706 (July 28, 2017) (presenting norms of state behavior in cyberspace).

6. Jason Healey & Tim Maurer, *What It'll Take to Forge Peace in Cyberspace*, CHRISTIAN SCI. MONITOR (Mar. 20, 2017), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/What-it-ll-take-to-forge-peace-in-cyberspace.

7. *See, e.g.*, Duncan B. Hollis, *China and the US Strategic Construction of Cybernorms: The Process Is the Product*, HOOVER INST. WORKING GRP. ON NAT'L SEC., TECH., & L., AEGIS SERIES PAPER NO. 1704, 2017 (discussing how cybernorms develop and function over time); Ashley Deeks, *Moving Forward on Cyber Norms Domestically*, LAWFARE (July 10, 2017, 1:10 PM),

cybersecurity firms and some governments have quantified and made public evidence regarding the breadth and depth of, malicious cyber infiltrations by state actors into the networks of foreign businesses and other governments.[8]

In thinking about doctrine to govern cyberspace and strategies to prevent cyber intrusion, one cannot ignore the cyber domain's interaction with other domains or the applicability of existing legal tools to address cyberspace issues.[9] This Comment focuses on the latter. It queries whether international economic law tools could serve a useful purpose in governing state-to-state cyber interactions, at least where those interactions pertain to national or international economic relations.

I argue that any discussion regarding deterrence and a playbook of consequences for cyber incidents by state actors ought necessarily to include a careful examination of existing plays, particularly where those incidents have an economic component, as many do. I maintain that current and available international economic tools offer significant potential to shape cyber activities and norms, and only now are beginning to be deployed this way.

The Comment focuses on three areas: first, multilateral institutions and the potential for their use; second, regional and bilateral trade and investment instruments; and third, unilateral tools available to the United States in working with other states on cyber issues. Where the United States and others have begun to use international economic tools to address cyber issues, I evaluate their success. State responsibility for economic cybersecurity is a dynamic and rapidly changing field as states experiment with these mechanisms, and is likely to continue to change even as this Comment goes to print. Nevertheless, it is useful to take stock of present and past initiatives with an eye to future potential.

II. OVERVIEW OF INTERNATIONAL ECONOMIC TOOLS

The focus of this symposium is deterrence, which raises two fundamental questions: deterrence against what and for whom? Further, the symposium seeks to design a playbook of consequences: responsive actions that can be taken following a cyber incident. In this sense, our group study concentrated on *post-hoc* deterrence across a wide spectrum of cyber activities directed at other bad state actors. Among

---

https://www.lawfareblog.com/moving-forward-cyber-norms-domestically (describing how to clarify and strengthen norms domestically).

8. *See, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (last visited Mar. 8, 2018) (detailing China's authorization of foreign cyber intrusion); OFFICE OF THE U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 (Mar. 22, 2018) (setting out evidence regarding China's cyber intrusions into U.S. businesses).

9. As Dorothy Denning has written, "Just as any attempt to develop a single deterrence strategy for all undesirable activity across the traditional domains would be fraught with difficulty, so too for cyberspace. Yet this is how many authors have approached the topic of deterrence in cyberspace. Instead, by focusing on particular cyber weapons that are amenable to deterrence or drawing from existing deterrence regimes, the issues become more tractable." Dorothy E. Denning, *Rethinking the Cyber Domain and Deterrence*, 77 JOINT FORCE Q. 8, 8–9 (2015).

other considerations, the ongoing discussion of cyber norms is intended to clarify what is appropriate cyber-behavior. Thereafter, when a state acts inconsistently with agreed norms, responsive actions by other states will deter later transgressions.

International economic law takes a different view of deterrence. In fact, very little scholarship speaks to the deterrence elements of international economic law.[10] To the extent that commentators have focused on deterrence in international economic law, it is often in respect of a potential chilling effect that certain international economic law measures could have on regulation.[11]

More attention has been paid in the international economic law regime to collective action deterrence by way of institutional growth in the last thirty years, alongside the growth in state cyber capabilities. Where those cyber activities have economic effects or purposes, international economic tools may provide a space for engagement with and, in certain cases, enforcement against offending state cyber actors. For example, among the commitments made by President Xi and President Obama was a statement that neither country would "conduct or knowingly support" cyber-enabled theft of trade secrets and confidential business information "with the intent of providing competitive advantages to their companies or commercial sectors."[12] Such activity is directly related to the economic security of both the United States and China, as well as the transnational commercial activity of both countries' businesses.

Leaders in the global effort to create norms for cyber activity have had to confront the same concepts as Frank Easterbrook advanced in a domestic context in 1996.[13] Easterbrook queried whether new legal concepts were necessary to govern activities in cyberspace.[14] To be sure, my goal is not to cover all the tools comprehensively, and such a short Comment would not permit me to do so; rather I will highlight certain tools, their use and non-use, and the potential for the future. Further, none of these tools is intended as a panacea for cyber issues. A multi-layered and comprehensive cyber engagement strategy exceeds the scope of this paper.

This Part surveys the multilateral, plurilateral, bilateral, and unilateral institutions available to states that both establish international obligations relevant to cyber economic activity and provide mechanisms for recourse against states that violate those obligations. It examines possible and existing tools that would buttress the normative commitments already in place and that are available to enforce those commitments.

---

10. Exceptionally, *see* Jeffrey Kucik & Krzysztof J. Pelc, *What Can Financial Markets Tell Us About International Courts and Deterrence?*, INT'L CTS. & DOMESTIC POL. (forthcoming June 2018) (describing the examination of deterrence by economic institutions as a novel approach).

11. *See, e.g.*, Vicki Been & Joel C. Beauvais, *The Global Fifth Amendment? NAFTA's Investment Protections and the Misguided Quest for an International "Regulatory Takings" Doctrine*, 78 N.Y.U. L. REV. 30, 39 (2003) (discussing negative effects that regulatory deterrence may have on the effectiveness of the North American Free Trade Agreement).

12. *Press Release*, The White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015); Barack Obama, President, The President's News Conference with President Xi Jinping of China (Sept. 25, 2015).

13. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

14. *See generally id.*

A. Multilateral Tools

The World Trade Organization (WTO) is likely the most significant multilateral or international organization for international economic law. The organization is run by its 164 member governments and administered by a Secretariat to which those governments have delegated some authority.[15] The WTO's foundation is a series of negotiated agreements that constitute trade rules for its members. These agreements start with broad principles for trade and include sector- or topic-specific rules including for cross-border services and intellectual property. There is no cyber-specific agreement and there is no doubt that the rules were not designed with cyber activity in mind. The WTO was created in 1994 at a time when the potential for cyber activity was largely unknown. Thus, the current trade rules are not designed to accommodate twenty-first century challenges, particularly with respect to cyberspace.

A critical component of the WTO—a paradigmatic collective deterrence institution[16]—is its dispute settlement mechanism.[17] All major world powers are active participants in the WTO dispute settlement system and, unlike other international dispute settlement mechanisms, most countries, including states that are active cyber operators, seek to comply with the WTO dispute settlement decisions.[18]

The WTO provides multiple opportunities for states to consider and deliberate on problematic domestic legislation and state behavior that relates to trade rules, including cyber related measures. For instance, in September 2017, at the WTO Council for Trade in Services, the United States—together with Japan, South Korea, Austrailia, and Chinese Taipei—criticized as a possible violation of the General Agreement on Trade in Services China's wide-ranging new cybersecurity law which required companies to disclose intellectual property to the government and store data locally to be allowed to operate in China.[19] China replied that safeguarding

15. *See generally The WTO*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/thewto_e.htm (last visited Feb. 24, 2018) (describing state membership to the WTO and its operational structure).

16. T.V. PAUL, PATRICK M. MORGAN & JAMES. J. WIRTZ, COMPLEX DETERRENCE: STRATEGY IN THE GLOBAL AGE 164 (2009).

17. *See generally Dispute Settlement*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/dispu_e/dispu_e.htm (last visited Feb. 24, 2018) (providing information on the purpose and procedures of the dispute settlement mechanism).

18. *See Legal Effect of Panel and Appellate Body Reports and DSB Recommendations and Rulings*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c7s1p1_e.htm (last visited Feb. 24, 2018) ("[T]he conclusions and recommendations . . . become binding upon the parties to the dispute.").

19. Council for Trade in Services, *Communication from the United States: Measures Adopted and Under Development by China Relating to Its Cybersecurity Law*, WTO Doc. S/C/W/374 (Sept. 26, 2017). *See also WTO Members Examine New Proposals for Domestic Regulation in Services*, WORLD TRADE ORG. (July 5, 2017),

cybersecurity is a legitimate regulatory right for each member.[20]

Nevertheless, David Fidler maintains that WTO members have not used the WTO dispute settlement mechanism to address certain cyber harms because of the "difficulty of formulating claims" that such measures violate WTO agreements.[21] Speaking specifically of a potential claim that the cyber behavior of a WTO member violated a WTO agreement, Fidler argues that "it is not clear that [another] WTO member could satisfy [the evidentiary] burden" of such a claim "by relying on evidence from private-sector entities."[22] As Fidler describes, while cybersecurity firms like Mandiant have documented malicious cyber-economic behavior by China,[23] governments have been more guarded.[24]

B. Regional or Bilateral Tools

Apart from its commitments under the WTO framework, the United States and most other states also maintain robust regional and bilateral economic agreements. In the last twenty years, some of these agreements have evolved to include actionable commitments specific to cyber issues and other commitments that may be applied to state-attributed cyber harms. I will briefly discuss two types.

Bilateral investment treaties (BITs) provide safeguards for investors making investments in foreign countries. Under the dispute settlement mechanisms of BITs, an investor may sue an infringing state or a state may sue another state party to the treaty. No publicly available investor-state decision appears to address cyber harms.[25] Further, nothing in the most recent (2012) U.S. Model BIT[26] speaks specifically to cyber harms, although that would not preclude an investor or state from bringing a case alleging harm to an investment through cyber intrusion.

Legislation known as Trade Promotion Authority (TPA)[27] serves as the

---

https://www.wto.org/english/news_e/news17_e/serv_11jul17_e.htm.

20. *WTO Members*, *supra* note 19.

21. David Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, ASIL INSIGHT, Mar. 20, 2013.

22. *Id.*

23. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (Feb. 9, 2013).

24. *But see* U.S. DEP'T OF JUSTICE, U.S. CHARGES FIVE CHINESE MILITARY HACKERS FOR CYBER ESPIONAGE AGAINST U.S. CORPORATIONS AND A LABOR ORGANIZATION FOR COMMERCIAL ADVANTAGE (2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

25. Based on a search for publically available investment decisions conducted on October 15, 2017. Some arbitral panels have considered and admitted documents obtained through computer hacking. *See, e.g.*, Brigitta John, *Admissibility of Improperly Obtained Data as Evidence in International Arbitration Proceedings*, KLUWER ARBITRATION BLOG (Sept. 28, 2016), http://arbitrationblog.kluwerarbitration.com/2016/09/28/admissibility-of-improperly-obtained-data-as-evidence-in-international-arbitration-proceedings/; Caratube Int'l Oil Co. and Mr. Devincci Salah Hourani v. Republic of Kazakhstan, ICSID Case No. ARB/13/13.

26. U.S. DEP'T ST., U.S. MODEL BILATERAL INVESTMENT TREATY (2012), https://www.state.gov/documents/organization/188371.pdf.

27. Bipartisan Congressional Trade Priorities and Accountability Act of 2015, Pub. L. No. 114-26 (2015) (TPA was last renewed in 2015).

foundation for all U.S. trade agreements of the last forty years. TPA sets out objectives and content for inclusion in trade agreements negotiated by the executive branch with U.S. trading partners. It includes, as of 2015, objectives in the areas of digital trade in goods and services and cross-border data flows. TPA seeks "to ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data."[28] For the first time among TPA statutes, the 2015 TPA legislation refers to the importance of "preventing or eliminating government involvement in the violation of intellectual property rights, including cyber theft and piracy."[29] As a result of this inclusion, the Trans-Pacific Partnership Agreement negotiated by the United States together with eleven other countries—but from which the United States has now withdrawn—includes robust electronic commerce and intellectual property chapters, which include specific provisions on cyber matters.[30]

The advantage of placing in trade and investment agreements obligations regarding cyber activity related to cross-border commerce, is that those commitments are likely enforceable by the parties to the agreement. That is, most binding commitments in U.S. trade agreements negotiated in recent years include state-to-state enforcement mechanisms through their dispute settlement chapters. While the United States has only commenced one dispute settlement proceeding pursuant to a trade agreement in the last twenty years (on a topic unrelated to cyber matters), the opportunity would be available where the agreements so provide. Thus, future trade agreements negotiated under TPA 2015, or future delegations of authority from Congress following the expiration of TPA 2015, could include the commitments outlined above, and the Office of the United States Trade Representative (USTR) and other agencies could innovate enforcement measures against U.S. trading partners.

C. Unilateral Tools

In addition to the multi- and plurilateral commitments described above, U.S. agencies could unilaterally undertake to use international economic tools codified in domestic law against offenders in their efforts to enforce cyber commitments. A trend in this direction began under the Obama administration, and has continued under the Trump administration.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) maintains numerous sanctions programs that target either countries or individuals and impose a type of embargo against dealings with those countries or individuals. The OFAC's authority to impose such sanctions is derived principally from the International Emergency Economic Powers Act (IEEPA), which authorizes

28. *Id.* § 102(b)(6)(C).

29. *Id.* § 102(b)(5)(A)(vi).

30. Trans-Pacific Partnership Agreement, arts. 14, 18, Feb. 2016, New Zealand treaty depository, available at https://www.mfat.govt.nz/en/about-us/who-we-are/treaties/trans-pacific-partnership-agreement-tpp/text-of-the-trans-pacific-partnership/.

the President to impose economic sanctions to respond to a national emergency.[31]

On April 1, 2015, President Obama invoked the IEEPA and the National Emergencies Act,[32] among other authorities, issuing an Executive Order to create a sanctions authority to be administered by OFAC for cyber activities.[33] The order blocks the transfer of property belonging to individuals engaging in "significant malicious cyber-enabled activities."[34] In the Order, the President concludes that "the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located . . . outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, *and economy* of the United States."[35] Emphasizing this link between the cyber activities of foreign actors and the economic security of the United States was not a new idea, but to have it highlighted at the highest levels of the government with significant effect gave the concept renewed authority and license for economic agencies throughout the government to operationalize cyber-focused efforts. The order goes on to speak to activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the "economic health or financial stability of the United States."[36] Where those activities have the purpose or effect of "causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain," the Secretary of the Treasury is empowered to take action to block the transfer of property of responsible individuals from within the United States to outside the United States.[37]

A significant development between the time of the May 2017 symposium and the moment this issue will go to press is the Trump administration's move away from sanctions[38] and the use instead of a tool from the Trade Act of 1974[39] (1974 Trade Act) to fight one type of malicious state-sponsored cyber economic activity.

The 1974 Trade Act set up a number of new or revised tools for private parties to take advantage of the U.S. domestic system where they were aggrieved by a foreign trade action. President Trump has sought to use Section 301 of the 1974 Trade Act after many years of nonuse.[40] The idea behind Section 301 is to permit

---

31. International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–06 (1977); *see* Perry S. Bechky, *Sanctions and the Blurred Boundaries of International Economic Law*, 83 MO. L. REV. (forthcoming 2018) (manuscript at 1) (describing the sanctions and how they operate).

32. 50 U.S.C. §§ 1601–51.

33. Exec. Order No. 13694, 80 Fed. Reg. 18,077 (Apr. 2, 2015).

34. *Id.*

35. *Id.* (emphasis added).

36. *Id.*

37. *Id.* On December 28, 2016, President Obama issued Executive Order 13757 that amended the first Order and specifically named several Russian individuals and entities which were accused of malicious cyber enabled activities. Exec. Order No. 13757, 82 Fed. Reg. 1, 3 (Jan. 3, 2017).

38. However, as of now, President Trump has maintained that there is a national emergency and that President Obama's Executive Orders are still in effect. *See* 163 CONG. REC. H2557 (daily ed. Mar. 29, 2017) (statement of President Trump).

39. Trade Act of 1974, Pub. L. No. 93-618 (as amended through Consolidated Appropriations Act, 2018, Pub. L. No. 115–141 (Mar. 23, 2018)).

40. *See* Chad P. Brown, *Rogue 301: Trump to Dust Off Another Outdated US Trade Law?*,

the United States to take action against trading partners that are unfairly burdening U.S. commerce. According to some observers, its utility today, given the creation of the WTO, is to bridge the gap between the WTO rules and areas not covered by those rules.[41] Section 301 also provides an opportunity for members of the public to force the government's consideration of a trade issue by including a mechanism for receiving a public petition,[42] something that I refer to as an "enforcement enhancement element," insofar as it permits public prompts for enforcement rather than leaving the commencement or pursuit of enforcement entirely to the executive branch.[43]

Although Section 301 is a tool that is employed by the United States acting alone, the European Union has a similar process. The European Union's analog to U.S. Section 301 is the Trade Barriers Regulation (TBR).[44] The TBR establishes a procedure enabling businesses and E.U. member states to request the E.U. institutions to examine any trade barriers put in place by non-E.U. states, to "safeguard the interests of E.U. companies and workers."[45] To date, the E.U. has initiated twenty-four cases under the TBR, the most recent of which was initiated in 2008.[46] Likewise, the last USTR-initiated investigation under Section 301 was initiated in 2010. Next, I describe how the Trump administration is seeking to use Section 301 to combat illicit cyber activity by China.

III. CURRENT USE OF INTERNATIONAL ECONOMIC TOOLS TO ADDRESS STATE CYBER ACTIVITIES

In the last three years, the United States has primarily pursued unilateral international economic law tools to combat malicious state-sponsored cyber activities. Applying tools from the international economic law toolkit requires a whole-of-government approach in which economic agencies collaborate with cyber experts, including those investigating possible attacks and enforcing criminal or national security commitments.

PETERSON INST. FOR INT'L ECON. (Aug. 3, 2017, 11:45 AM), https://piie.com/blogs/trade-investment-policy-watch/rogue-301-trump-dust-another-outdated-us-trade-law (explaining how the Trump administration can use this section in response to Chinese cyber intrusion).

41. *See* Bruce Hirsh, *Taking Matters into Your Own Hands - Section 301 of the Trade Act of 1974*, TRADE VISTAS (Aug. 3, 2017), https://tradevistas.csis.org/taking-matters-hands-section-301-trade-act-1974/ (explaining why the United States may consider using Section 301 rather that the WTO trade dispute mechanism).

42. *See* Trade Act of 1974, Pub. L. No. 93-618 (as amended), §§ 221–25 (stating requirements for petition).

43. *USTR Announces Initiation of Section 301 Investigation of China*, OFFICE OF THE U.S. TRADE REPRESENTATIVE (Aug. 18, 2017), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/august/ustr-announces-initiation-section.

44. Council Regulation (EC) No. 3286/94 of 22 December 1994.

45. *See* Eur. Comm'n Press Release IP/12/1390, Commission Proposes Improved Rules to Enforce EU Rights Under International Trade Agreements (Dec. 18, 2012).

46. EUR. COMM'N, GENERAL OVERVIEW OF ACTIVE WTO DISPUTE SETTLEMENT CASES INVOLVING THE EU AS COMPLAINANT OR DEFENDANT AND OF ACTIVE CASES UNDER THE TRADE BARRIERS REGULATION (Jan. 2018), http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154243.pdf.

In March 2017 and again in March 2018, President Donald Trump announced the continuation of the national emergency necessitating the cyber sanctions authority, but the government has exercised its authority sparingly.[47] Thus, the United States has not used the full extent of its sanctions power to hold accountable any state actors other than the Russian individuals and entities believed to be responsible for meddling in the 2016 presidential election and certain Iranian actors.

To be sure, the specialized cyber sanctions have a limited scope. The two Executive Orders require attribution to a group or individual. Given that precise attribution in cyberspace is challenging, the Secretary of the Treasury has the discretion to rely upon whatever degree or level of attribution he feels appropriate to exercise the authority accorded him by the president. The attribution analysis would need to be provided to the Treasury from another part of the government, requiring both close collaboration and consensus. Further, putting a state-related entity on a sanctions list—like any action against a foreign state—involves many political calculations.

It may be that the difficulties associated with applying sanctions led President Trump, on August 14, 2017, to take a different route in respect to China's cyber- and other technology-related activities. On that date, by memorandum, the President directed the USTR to determine in accordance with Section 301 of the 1974 Trade Act "whether to investigate any of China's laws, policies, practices, or actions that may be unreasonable or discriminatory and that may be harming American intellectual property rights, innovation, or technology development."[48] Four days later, the USTR initiated such an investigation.[49]

China is familiar with the U.S. unilateral actions under Section 301 and its affiliated parts of the 1974 Trade Act. In 1991, the USTR initiated such an investigation with respect to certain acts, policies, and practices of China that, according to the United States, "deny adequate and effective protection of intellectual property rights."[50] Throughout the 1990s, the USTR and the Chinese government engaged closely on these issues.[51]

The USTR's 2018 Section 301 investigation, which preliminarily concluded several months before the statutory deadline with the issuance of an extensive report

47. 163 Cong. Rec. H2557 (daily ed. Mar. 29, 2017) (statement of President Trump maintaining the national emergency declared by President Obama); THE WHITE HOUSE, NOTICE REGARDING THE CONTINUATION OF THE NATIONAL EMERGENCY WITH RESPECT TO SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES (Mar. 27, 2018).

48. Donald J. Trump, Presidential Memorandum for the United States Trade Representative (Aug. 14, 2017). The Memorandum declares at the outset that China has "taken actions related to intellectual property, innovation, and technology, that may . . . negatively affect American economic interests."

49. *USTR Announces Initiation of Section 301 Investigation of China*, OFFICE OF THE U.S. TRADE REPRESENTATIVE (Aug. 18, 2017), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/august/ustr-announces-initiation-section.

50. Notice of Initiation of Investigation under Section 302(b)(2)(A) of the Trade Act of 1974, 56 Fed. Reg. 24877, 24878 (May 31, 1991).

51. *See generally* WAYNE M. MORRISON, CONG. RESEARCH SERV., CHINA-U.S. TRADE ISSUES (Jan. 23, 2018), https://fas.org/sgp/crs/row/RL33536.pdf.

by the USTR on March 22, 2018,[52] was not limited to cyber-enabled activity from China directed toward the United States. The investigation also reviewed Chinese laws and regulations that require U.S. businesses to share valuable technical information with Chinese authorities to invest or operate in China. Further, as noted, the investigation process under Section 301 invites comments from the public on the topic. A public hearing was held on October 10, 2017, in which the USTR and other agencies received information from the private sector on the extent of Chinese activity.[53] Although the USTR concluded that China's activities rose to the level of the statute, the U.S. government was still considering at the time this Comment goes to print the scope of the remedy to be applied. The range of remedies that the government chooses to employ in this process will test the utility of the U.S. unilateral instruments against malicious state-sponsored cyber activity.

A strong op-ed from the former director of national intelligence and the former commander of the United States Cyber Command and the National Security Agency followed the President's August 2017 announcement.[54] In their column, Director Dennis Blair and Commander Keith Alexander asserted that the effort by the Trump administration was long overdue and that China has been engaged in a "decades-long assault on the intellectual property of the United States and its allies."[55] But while Blair and Alexander supported the President's move, trade experts had a different reaction. Jim Bacchus, former chairman of the Appellate Body of the WTO, made public statements suggesting that the United States should use the WTO for an action against China with economic implications rather than unilateral actions.[56] Noting that it would be challenging to do so, Bacchus commented that such an action would benefit from an international imprimatur.[57]

IV. RECOMMENDATIONS FOR THE FUTURE USE OF INTERNATIONAL ECONOMIC TOOLS TO ADDRESS STATE CYBER ACTIVITIES

While the efforts of the Trump administration to seek to apply existing international economic tools to combat state-sponsored cyber activity is a step in the right direction, more can be done and much remains to be seen.

---

52. OFFICE OF THE U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 (Mar. 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

53. Notice of Initiation of Investigation; Hearing; and Request for comments, 82 Fed. Reg. 40213 (Aug. 24, 2017).

54. Dennis C. Blair & Keith Alexander, Opinion, *China's Intellectual Property Theft Must Stop*, N.Y. TIMES (Aug. 15, 2017), https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html. Joel Brenner raised the alarm long ago, as did others. *See, e.g.*, Joel Brenner, *The New Industrial Espionage*, AM. INTEREST (Dec. 10, 2014), https://www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/.

55. Blair & Alexander, *supra* note 54.

56. *See, e.g.*, James Bacchus, Opinion, *How to Take on China Without Starting a Trade War*, WALL ST. J. (Aug. 16, 2017), https://www.wsj.com/articles/the-u-s-doesnt-have-to-take-on-china-alone-1502904996.

57. *Id.*

First, thus far, the United States has focused on China given China's well-known conduct in using cyber means to obtain sensitive business information from foreign businesses. Unlike other areas of international law, international economic law is an area in which China is active and responsive. For this reason, testing these tools on China makes good sense. Policymakers across the U.S. government should continue to invest resources in the use of international economic institutions for addressing Chinese state cyber activity.

But, second, U.S. application of just one potential trade enforcement mechanism (Section 301) is not enough with respect to scope (China only), and it remains too early to evaluate. More should be done to think creatively about how this mechanism can be deployed against other actors, where appropriate, for other cyber economic activity as the Section 301 action continues to evolve. A full evaluation will be necessary following the USTR's implementation of remedies in response to its March 2018 report.

Third, policymakers should consider multilateral and plurilateral tools either in addition to or in place of the unilateral tools. In respect of cyber activity, the strongest legal weapons should be deployed.

Policymakers should consider adding express provisions to free trade agreements and bilateral investment treaties that can accommodate claims about economic harms through cyber activities. This option would create specialized mechanisms with a mandate to police this type of activity with the enforcement authority to impose trade sanctions where necessary. The provisions could also provide opportunities for experts in cyber activity to serve as panel members together with trade or investment experts or for such experts to be appointed specially for review of technical evidence. A dispute settlement system built into forthcoming agreements would be consistent with congressional interest and international norms, and would provide a neutral forum for resolving such issues thereby promoting the rule of law in both economic and cyber contexts. Economic and cyber issues have multiple points of intersection. Managing those intersections requires further legal development.

The use of a standing dispute body or arbitration panels created under standing trade instruments would help depoliticize cyber economic issues in a way that also can lead to effective enforcement of international obligations. Making a clear statement as to the prohibition of cyber economic espionage and related activity in enforceable trade instruments would be the first and next step to successfully applying these tools.

V. CONCLUSION

As international lawyers, we can too easily dismiss collective action options for deterrence in the absence of an international body dedicated to the subject. However, in recent history, states are accustomed to creating new institutions to address new threats or old problems with new interest. This Comment has sought to use existing international organizations to achieve the same. At a minimum, adding international economic institutions to a playbook designed to fight malicious state-sponsored cyber activity is prudent given their chances for success in changing state behavior when seemingly very little else will.