

Cornell International Law Journal

Volume 51
Number 2 *Spring 2018*


Article 4

“Private” Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime

Shin-yi Peng

National Tsing Hua University, Taiwan

Follow this and additional works at: <https://scholarship.law.cornell.edu/cilj>

 Part of the [Computer Law Commons](#), [International Law Commons](#), [International Trade Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Peng, Shin-yi (2018) ““Private” Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime,” *Cornell International Law Journal*: Vol. 51 : No. 2 , Article 4.

Available at: <https://scholarship.law.cornell.edu/cilj/vol51/iss2/4>

This Article is brought to you for free and open access by the Journals at Scholarship@Cornell Law: A Digital Repository. It has been accepted for inclusion in Cornell International Law Journal by an authorized editor of Scholarship@Cornell Law: A Digital Repository. For more information, please contact jmp8@cornell.edu.

“Private” Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime

Shin-yi Peng†

Introduction

An increasingly connected world has brought more sophisticated cybersecurity threats. Although not all instances are disclosed, outbreaks of cyber hacks on governments and companies have been featured in the headlines in recent years. Yahoo! Inc., for example, lost more than 500 million user accounts,¹ which “may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers.”² The breaches forced Yahoo to renegotiate its sale to Verizon Communications Inc., cutting the price by \$350 million.³ In a similar case, the Information Commissioner’s Office (ICO) of the UK slapped Telecom’s TalkTalk with a record £400,000 fine for failing to keep personal data secure, which “allowed cyber attackers to access customer data ‘with ease.’”⁴

† Professor of Law, National Tsing Hua University, Taiwan. An earlier version of this Article was presented at the European Society of International Law (ESIL) Annual Conference “*Global Public Goods, Global Commons and Fundamental Values: The Responses of International Law*,” Naples, Italy, on 7-9 September 2017. I thank the participants at the ESIL Conference for their comments.

1. Mark Fahey & Nick Wells, *Yahoo Data Breach Is Among the Biggest in History*, CNBC (Sept. 26, 2016, 11:19 AM), <http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html> [<https://perma.cc/RL7F-5LWN>].

2. Yahoo Security Notice December 14, 2016, YAHOO, <https://help.yahoo.com/kb/SLN27925.html> (follow “What information was taken in the August 2013 incident?” drop-down option) [<https://perma.cc/3W6V-JY8Q>].

3. Michael Liedtke & Tali Arbel, ASSOCIATED PRESS, *Yahoo Salvages Verizon Deal with \$350 Million Discount*, YAHOO FINANCE (Feb. 21, 2017), <https://finance.yahoo.com/news/yahoo-salvages-verizon-deal-350-132641836.html> [<https://perma.cc/8UC7-PWLH>].

4. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers, and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes. The ICO’s investigation found that an attack on the company could have been prevented if TalkTalk had taken basic steps to protect customers’ information. ICO (UK) News, *Talktalk Gets Record £400,000 Fine for Failing to Prevent October 2015 Attack* (Oct. 5, 2016), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/> [<https://perma.cc/L5MA-4F5R>]; see also Keely Rushmore, *ICO Issues Record £400,000 Monetary Penalty Notice for Talktalk Data Breach*, SA LAW (Dec. 20, 2016), [https://salaw.com/views-insight/keely-rushmore-](https://salaw.com/views-insight/keely-rushmore-51)

These examples signal a clear desire for stronger personal data security. The range of consequences for security failures are substantial, including civil financial losses and even criminal liabilities. We are now living in a hyper-connected world, with a myriad of devices continuously linked to the Internet. Our growing dependence on such devices exposes us to a variety of cybersecurity threats.⁵ This ever-increasing connectivity means that vulnerabilities can be introduced at any phase of the software development cycle.⁶ Cybersecurity risk management, therefore, is more important than ever to governments at all developmental stages as well as to companies of all sizes and across all sectors.⁷ The awareness of cybersecurity threats affects the importance placed on the use of standards and certification as an approach.⁸

Establishing cybersecurity standards enhances security and contributes to risk management by helping to establish common security requirements and capabilities needed for secure solutions.⁹ While it is impossible to eliminate all threats, cybersecurity standards make it harder for attacks, or at least reduce the effect of attacks that do occur.¹⁰ The overall goal of cybersecurity standards is to improve the security of information technology systems, networks, and critical infrastructures.¹¹ Typically, cybersecurity standards define functional and assurance requirements, policies for managing information, criteria for evaluating security measures, techniques for addressing security failures, and procedures for the monitoring of security breaches.¹² Technically speaking, such standards are very diverse, ranging from the mathematical definition of a cryptographic algorithm to the specification of security features in a web browser.¹³ Ide-

emp-ico-issues-record-400000-monetary-penalty-notice-for-talktalk-data-breach/ [https://perma.cc/9ZKJ-CV83].

5. See E.U. AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Governance Framework for European Standardization* 8 (July 1, 2016), <https://www.enisa.europa.eu/publications/policy-industry-research> [https://perma.cc/354C-U59U].

6. See RICHARD A. CLARKE & ROBERT KNAKE, *CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT* 69–83 (2012); see generally Rolf H. Weber, *Internet of Things: New Security and Privacy Challenges*, 26 *COMPUTER L. & SECURITY REV.* 23 (2010). See generally P.W. SINGER & ALLAN FRIEDMAN, *CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW* 34 (2014).

7. E.U. AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Definition of Cybersecurity—Gaps and Overlaps in Standardisation* 8 (July 1, 2016), <https://www.enisa.europa.eu/publications/definition-of-cybersecurity> [https://perma.cc/F5AY-3XW4]. See generally Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18 *J. OF INT'L ECOM. L.*, 449 (2015).

8. PWC & DEP'T. FOR BUSINESS, INNOVATION AND SKILLS (BIS), *UK CYBER SECURITY SKILLS RESEARCH REPORT 4* (Nov. 2013), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf [https://perma.cc/P4KW-CBFF].

9. See generally William Stallings, *Standards for Information Security Management*, 10 *INTERNET PROTOCOL J.* 10 (2007).

10. *Id.*

11. *Id.*

12. See also INT'L ORG. FOR STANDARDIZATION (ISO), *ISO/IEC 27001:2013*, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v:1:en> [https://perma.cc/Z883-AE63] (last visited Aug. 12, 2018).

13. *Id.*

ally, “security standards facilitate sharing of knowledge and best practices by helping to ensure common understanding of concepts, terms, and definitions, which prevents errors.”¹⁴ On the other hand, “when cybersecurity standards are not available . . . [businesses] may not have reliable information . . . on what . . . security controls may be needed . . . [which] tends to lead to . . . insufficient security maintenance” if not unsafe implementations.¹⁵

It should be noted that this research focuses on international trade in goods rather than trade in services.¹⁶ While estimates vary, experts foresee that, by 2020, the Internet of Things (IoT) will connect 26 billion devices worldwide.¹⁷ The large-scale use of IoT technologies could have a range of implications and create various trade issues.¹⁸ Among other issues, greater technical standardization can reduce the barriers to entry to IoT markets. To illustrate, if devices from different manufacturers do not use the same cybersecurity standards, interoperability will require extra gateways to translate from one standard to another.¹⁹ Without effective

14. KAREN SCARFONE, DAN BENIGNI, TIM GRANCE, NIST, *CYBER SECURITY STANDARDS* (2009), available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152153 [<https://perma.cc/H8JZ-NZJK>].

15. *Id.* See generally Marjory S. Blumenthal, *Finding Security in the Clouds*, in *REGULATING THE CLOUD: POLICY FOR COMPUTING INFRASTRUCTURE* 61-86 (Christopher S. Yoo & Jean-François Blanchette eds., 2015).

16. However, this research does not aim to cover the rules of the GATS. Thus, Chapter IV does not deal with cybersecurity standards in the context of trade in services, i.e., GATS Article VI:5(a). According to the negotiating papers, “technical standards” are measures that lay down the characteristics of a service or the manner in which it is supplied. Technical standards also include the procedures relating to the enforcement of such standards. Domestic cybersecurity regulation is therefore arguably a “technical standard” within the meaning of Article VI:4/5. See Working Party on Domestic Regulation, *Disciplines on Domestic Regulation Pursuant to GATS Article VI:4*, Informal Note by the Chairman, Room Document, 20 March 2009, para. II:5, available at https://www.southcentre.int/wp-content/uploads/2013/08/AN_SV12_The-Draft-GATS-Domestic-Regulation-Disciplines_EN.pdf [<https://perma.cc/74Z6-LN2P>] (last visited Aug. 12, 2018). For cybersecurity issues under the GATS, see Shin-yi Peng, *Digitalization of Services, the GATS and the Protection of Personal Data*, in *KOMMUNIKATION: Festschrift für ROLF H. WEBER ZUM 60. GEBURTSTAG [COMMUNICATIONS: LIBER AMICORUM FOR PROF. DR. ROLF H. WEBER]* 753, 753-69 (Reto M. Hilty et al. eds., 2011). See also Rolf Weber, *Regulatory Autonomy and Privacy Standards Under the GATS*, 7 *ASIAN J. WTO & INT’L HEALTH L. AND POL’Y*, 25, 26-47 (2012).

17. U.S. Dep’t of COMMERCE INTERNET POLICY TASK FORCE & DIG. ECON. LEADERSHIP TEAM, *FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS* 4 (2017), available at https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf [<https://perma.cc/6H4C-T3LK>].

18. IoT refers to “a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers.” RON DAVIES, EUROPEAN PARLIAMENTARY RESEARCH SERV., *THE INTERNET OF THINGS: OPPORTUNITIES AND CHALLENGES* 1-2 (2015). The IoT should be seen as the aggregation of many machine to machine (M2M) connections which focuses on the “sharing of data” and processing that takes place between these devices. See *id.*; see also FEDERAL TRADE COMMISSION (FTC), *CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS* (2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things> [<https://perma.cc/3PEM-9UJ8>].

19. See DAVIES, *supra* note 18, at 4.

standards, it will be difficult for small and medium-sized enterprises (SMEs) to enter the market. That said, the central issue here is whether the regulation of cybersecurity standards should follow a so-called “multistakeholder” approach, which, as discussed in this Article, has been championed over the years in the arena of Internet governance, or move towards a more multilateral approach in which states play central roles. Debates regarding Internet governance have long embodied a tension between positions advocating for greater government oversight of the Internet and those advocating for a coordinated structure spanning government, the private sector, and civil society.²⁰ Indeed, we are at a crossroads in global governance.²¹ The ongoing shift from multilateralism to multistakeholderism raises pivotal issues concerning cybersecurity norm development, namely—what is the appropriate role of the government in regulating the Internet? Is the multistakeholder approach effective and efficient in terms of norm creation and harmonization? Can existing informal cyberspace norms meet the goal as well as traditional, legally binding regulation? At a more fundamental level, why is the shift to multistakeholder governance happening? This Article will engage in arguments regarding questions about how to save the World Trade Organization (“WTO”) from the risk of irrelevance in the context of cyberspace governance, as well as how private cybersecurity standards can be regulated by the Agreement on Technical Barriers to Trade (the “TBT Agreement”).

I. The Standards Jungle of Cybersecurity

A. The Top-Down Approach: A Government-Centered Cybersecurity Standardization System

The implications of “standards” are different in various contexts.²² There is a strong relationship between national technical standards and an efficient international trading system. In a globalized world, standards pro-

20. See CTR. FOR INT’L GOVERNANCE INNOVATION AND THE ROYAL INST. OF INT’L AFFAIRS, WHO RUNS THE INTERNET? THE GLOBAL MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE 19-44 (2016); Joost Pauwelyn, *Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How They May Outcompete WTO Treaties*, 17 J. INT’L ECON. L. 739, 745 (2014); see generally Urs Gasser et al., *Multistakeholder as Governance Groups: Observations from Case Studies* (The Berkman Ctr. for Internet & Soc’y at Harv., Res. Publication No. 2015-1 (2015)); Scott J. Shackelford et al., *Bottoms Up: A Comparison of “Voluntary” Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 257 (2016); Shin-yi Peng, *The Soft Law Approach to Regulatory Harmonization: Are We Trading away Privacy for Economic Integration?* in A LIBER AMICORUM: MITSUO MATSUSHITA, A CRITICAL ASSESSMENT OF THE INTERNATIONAL ECONOMIC LAW AND GOVERNANCE 328, 335 (Julien Chaisse et al. eds., 2016); Alessandra Arcuri, *The TBT Agreement and Private Standards*, in RESEARCH HANDBOOK ON THE WTO AND TECHNICAL BARRIERS TO TRADE 485, 487 (Tracey Epps et al. eds., 2013).

21. See Petros C. Mavroidis & Robert Wolfe, *Private Standards and the WTO: Reclusive No More*, 16 WORLD TRADE REV. 1, 2-3 (2017).

22. See Shin-yi Peng, *Standards as a Means to Technological Leadership? China’s ICT Standards in the Context of the International Economic Order*, in CHINA IN THE INTERNATIONAL ECONOMIC ORDER: NEW DIRECTIONS AND CHANGING PARADIGMS 128 (Lisa Toohey et al. eds., 2015).

vide information about products to consumers in the importing country to ensure technical compatibility.²³ By sharing a common standard, anonymous manufacturers in markets all over the world can communicate, establish common expectations of one another's products, and evaluate the compatibility of their joint productions.²⁴ That said, cybersecurity standards can have a strong influence over "trade flow," as they affect the demand and supply of ICT goods and services.²⁵

In this context, perhaps China's top-down, government-centered standardization system represents the most outstanding case. In the Chinese ICT market, the government assumes primary responsibility in standardization development, with the policy rationale that state-led standardization creates the most efficient national economy.²⁶

China's Wireless LAN Authentication and Privacy Infrastructure ("WAPI") Standard, which was developed under a typical top-down government-central standardization system, demonstrates how cybersecurity standards might create effective trade barriers. The Institute of Electrical and Electronics Engineers ("IEEE") 802.11 Wi-Fi standard became the formal international standard of the International Organization for Standardization ("ISO"). However, the Chinese government decided to use a different "security" protocol, i.e., WAPI, for mandatory compliance.²⁷ Under the mandated Chinese approach, equipment vendors who sell WLAN devices in China must offer products based on the Chinese standard. China's approach to using technical regulations and standards in the ICT sector, which in many instances appears to have been designed to favor China-specific approaches, has caused substantial concerns. Industry associations have consistently encouraged the Chinese government to harmonize its standards regime with internationally recognized market-driven standards instead of creating its own.²⁸

The question as to whether the regulations China has developed in the cybersecurity area are consistent with WTO obligations remains unanswered.²⁹ Consequently, the Chinese ICT standards create a systematic increase in uncertainty and negatively impacts international trade. Earlier this year, more than 50 business groups from all over the world urged

23. *Id.* at 129; see also Xiaomeng Lu, *Standards-Related Barriers to Trade in Chinese ICT Market* (MONTEREY INST. OF INT'L STUDIES, Capstone Project Prepared for the MAITP Degree 7 (2008)).

24. *Id.*

25. Peng, *supra* note 22, at 144.

26. See DAN BREZNITZ & MICHAEL MURPHREE, U.S.-CHINA ECON. AND SEC. REVIEW COMM'N, *THE RISE OF CHINA IN TECHNOLOGY STANDARDS: NEW NORMS IN OLD INSTITUTIONS* 2 (2016).

27. See Christopher S. Gibson, *Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards*, 22 BERKELEY TECH. L.J. 1403, 1435 (2007).

28. See DIETER ERNST, UC INST. ON GLOB. CONFLICT AND COOPERATION AND THE EAST-WEST CTR., *INDIGENOUS INNOVATION AND GLOBALIZATION: THE CHALLENGE FOR CHINA'S STANDARDIZATION STRATEGY* 67 (2011).

29. See Peng, *supra* note 22, at 145.

China to delay the enforcement of its new cybersecurity law,³⁰ which was slated to take effect on June 1, 2017. The group stressed that the new cybersecurity law, especially those measures that require the use of secure and controllable technologies in the ICT sector, as well as future implementation standards, will effectively erect trade barriers and thus “adversely impact billions of dollars in cross-border trade.”³¹ The recent “trade war under the guise of cybersecurity” raises the question of how top-down approaches to standardization can better ensure China’s cybersecurity without sacrificing the benefits of global trade.³²

B. The Bottom-Up Approach: Multistakeholder Platforms for Cybersecurity Standardization

There exists a spectrum of cybersecurity standardization models, ranging from more centralized governmental involvement, such as in the case of China, to more decentralized private initiatives. The reality is that a “traditional” top-down regulatory approach now struggles to keep pace with the innovation on the Internet. There is a growing trend across the world toward a bottom-up approach to cybersecurity standardization.³³ Empirical studies demonstrate that more and more jurisdictions have been settling on a bottom-up approach to cybersecurity policymaking, which aims to minimize mandatory governmental regulation and to favor a voluntary, private-sector standard to enhance cybersecurity.³⁴ Under the bottom-up approach, the business sector has actively taken on the standardization initiative, which they contend leads to more cost-effective rules than government regulation.³⁵ This privatization of governance is driven, in part, by governments’ lack of requisite technical expertise and the flexibility to deal with ever-more complex regulatory tasks.³⁶ The

30. ASSOCIATED PRESS, *Global Business Groups Urge Beijing to Delay Cybersecurity Law*, SOUTH CHINA MORNING POST (May 15, 2017), <http://www.scmp.com/news/china/article/2094450/global-business-groups-urge-beijing-delay-cybersecurity-law> [https://perma.cc/9BMF-QUT3]; see also Letter from ACT: The App Association, et al., to Chinese Communist Party Central Leading Group for Cyberspace Affairs (May 15, 2017) (on file with author); Rick Weber, *U.S. Commission Echoes Industry Concerns About Broad Scope of China’s New Cybersecurity Law*, INSIDE CYBERSECURITY (Aug. 22, 2017), <https://insidecybersecurity.com/daily-news/us-commission-echoes-industry-concerns-about-broad-scope-chinas-new-cybersecurity-law> [https://perma.cc/L92L-3MBE].

31. Michael Martina & Cate Cadell, *Amid Industry Pushback, China Offers Changes to Cyber Rules: Sources*, REUTERS (May 19, 2017), <https://www.reuters.com/article/us-china-cyber-law/amid-industry-pushback-china-offers-changes-to-cyber-rules-sources-idUSKCN18F1VZ> [https://perma.cc/EZ7J-BQ77]. The group also underscored the asymmetry between the access that foreign countries are granted to China’s ICT market and the access Chinese companies enjoy in other markets.

32. WORLD TRADE ONLINE, *Cybersecurity Claims Mask Ongoing U.S.-China ‘Trade War’ over Tech Products*, INSIDE U.S. TRADE (July 13, 2017), <https://insidetrade.com/trade/cato-paper-cybersecurity-claims-mask-ongoing-us-china-trade-war-over-tech-products> [https://perma.cc/73DF-QLTN].

33. Shackelford, *supra* note 20, at 259.

34. *Id.*

35. TIM BUTHE ET AL., *THE NEW GLOBAL RULERS: THE PRIVATIZATION OF REGULATION IN THE WORLD ECONOMY* 5 (2011).

36. *Id.*

involvement of public and private sector actors working together has proven to be a more effective model than complete government control.

Emblematic of this movement in the context of the European Union is the European Union Agency for Network and Information Security (“ENISA”).³⁷ Since its founding in 2004, ENISA has actively contributed to cybersecurity standards and thus to proper functioning of the internal market within the Union.³⁸ By working closely together with the EU member states and the private sector, ENISA provides advice and solutions related to cybersecurity, supports policy implementation, and coordinates standardization activities.³⁹ As ENISA repeatedly stresses in its policy papers, it believes enhancing the role of public-private partnerships should be emphasized in standardization processes.⁴⁰ A bottom-up approach to the creation of cybersecurity standards and strong representation from stakeholders are the key elements in ENISA decision-making procedures.⁴¹

On the other side of the Atlantic, the U.S. National Institute for Standards and Technology Cybersecurity Framework (the “NIST Framework”) represents another striking example of a bottom-up approach to cybersecurity standardization. The NIST, now a part of the U.S. Department of Commerce, is one of the nation’s oldest physical science laboratories.⁴² To respond to Executive Order 13636, issued in February of 2013, the NIST utilized a year-long consultative process with stakeholders to create the NIST Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks.⁴³ In a series of multi-stakeholder meetings, hundreds of international representatives from govern-

37. See generally EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, <https://www.enisa.europa.eu/> [<https://perma.cc/4HVU-H92T>] (last visited Aug. 12, 2018) (ENISA is a center of expertise for cyber security in Europe).

38. See EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *About ENISA*, <https://www.enisa.europa.eu/about-enisa> [<https://perma.cc/4XP7-P4YZ>] (last visited Aug. 12, 2018).

39. *Id.*

40. *Id.*

41. See *id.*; see also EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, GOVERNANCE FRAMEWORK FOR EUROPEAN STANDARDISATION 19 (2015) (stating that “Cybersecurity standards should be created based on the needs of stakeholders. Appropriate entities should collect the relevant information on the need of standardization activities through public consultations with the industry, research and supervisory bodies.”).

42. US DEP’T OF COMMERCE, *About NIST*, <https://www.nist.gov/about-nist> [<https://perma.cc/CPJ7-ZUYU>] (last visited Aug 12, 2018).

43. US DEP’T OF COMMERCE, *Cybersecurity Framework*, <https://www.nist.gov/cyber-framework> [<https://perma.cc/N3BK-W84T>] (last visited Aug. 12, 2018). The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. See NAT’L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), available at <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf> [<https://perma.cc/RCN4-W5Y3>] (providing contextual background on the Executive Order and the Cybersecurity Framework); see also Lei Shen, *The NIST Cybersecurity Framework: Overview and Potential Impacts*, 10 TECH. LAWYER 16, 17 (2014); Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT’L L.J. 305, 305 (2015).

ment, business, and civil society came together to create the NIST Framework.⁴⁴ Such a process demonstrates an active dialogue that relies on a bottom-up approach to cybersecurity regulation—building consensus across sectors and industries through a dynamic public-private partnership.⁴⁵ The NIST has continued to engage with stakeholders through multiple avenues of communication. Although now playing an active and central role in implementing the Trump administration's cybersecurity agenda,⁴⁶ the 2017 NIST Framework reaffirms its commitment to private sector self-governance.⁴⁷ Arguably, the international community needs some degree of governmental involvement in implementing standards to properly evaluate businesses' efforts, to incentivize private sector self-governance, and to reward stakeholders that meet those standards. Such a two-fold approach to public-private co-governance represents a compromise between top-down regulatory interference and outright self-governance.⁴⁸

Of course, the idea of governance through public-private networks is not new at all. Researchers, including those in international economy law, have long researched the changing role of the state in market economies and the transformation of public functions. Professor Shaffer, in his book, elaborates on how public hierarchies and private markets complement one another.⁴⁹ As Shaffer indicates, these networks bring together public and private actors to address policy issues.⁵⁰ In a world of increasing complexity, governments are delegating traditionally public functions to the private sector. Therefore, the world is increasingly governed through co-regulation by public and private actors.⁵¹ In the context of cybersecurity, where public and private sectors attempt to adapt to rapid technological changes, it is particularly evident that governments must relax the regulatory power and shift responsibility through privatization.

However, procedure and substance are often closely intertwined, as well as mutually defining. Due to the bottom-up approaches, cybersecurity standards are proliferating.⁵² A growing number of organizations are becoming involved in standards development, as more and more manufacturers and vendors build and sell standards-compliant products and ser-

44. Shackelford, *supra* note 20, at 222.

45. *Id.*

46. Rick Weber, *NIST Emerges as Key Player in Implementing Trump's Cybersecurity Agenda*, INSIDE CYBERSECURITY (July 3, 2017), <https://insidocybersecurity.com/daily-news/nist-emerges-key-player-implementing-trumps-cybersecurity-agenda> [https://perma.cc/X3SP-SA9F].

47. See generally US DEP'T OF COMMERCE, CYBERSECURITY FRAMEWORK WORKSHOP 2017 SUMMARY (2017), https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf [https://perma.cc/W66M-5AMA].

48. See generally US DEP'T OF COMMERCE, *supra* note 42.

49. GREGORY SHAFFER, DEFENDING INTERESTS: PUBLIC-PRIVATE PARTNERSHIPS IN WTO LITIGATION 12-14 (2003).

50. *Id.* at 12-13.

51. Shackelford, *supra* note 20, at 219.

52. SCARFONE ET AL., *supra* note 14 at 1.

vices.⁵³ To date, the number of cybersecurity standards, in some form, exceeds 1,000 publications globally,⁵⁴ resulting in a complex standards landscape. This “mushrooms after rain” phenomenon of private cybersecurity standards may lead to potential problems. Although, on the one hand it manifests the dynamics of the industry, it might also result in the danger of overlapping work. From the perspective of international trade, such diversity makes compliance challenging and therefore directs resources away from more effective mechanisms.⁵⁵ The international “standards jungle” of cybersecurity, as a result, may in fact work as an impediment to free trade.

II. Harmonization of Cybersecurity Standards

“[Differences in] standards matter little when markets are predominantly domestic.”⁵⁶ As shown in <Figure 1>, from the aspects of the top-down standardization approach, centralization may solve the problems of duplication and fragmentation. The advantage of a centralized, non-market, public standard-setting regime (Type I) is that the government can simply mandate the adoption of non-competing cybersecurity standards as *de jure* technical regulations within the appropriate jurisdiction when the public sector plays a major role in the standard-setting process.⁵⁷ When a government adopts *de jure*, mandatory cybersecurity standards,⁵⁸ it can effectively prevent standards wars within the specific jurisdiction.

The integration of ICT markets, however, has greatly increased interdependence and has thus created incentives to coordinate on common technical solutions.⁵⁹ By standardizing different, but otherwise incompatible products, “international standards” have contributed to the enhancement of economic globalization.⁶⁰ Standards provide information about products to consumers in the importing country to ensure technical compatibility.⁶¹ By sharing a common standard, anonymous manufacturers in markets all over the world can benefit from common expectations of one another’s products. The use of standards reduces uncertainty, because any innovator in the market can develop new applications with the guarantee

53. *Id.*

54. PWC & DEF’T. FOR BIS, *supra* note 8, at 4.

55. See Paula Bruening, *Interoperability: Analyzing the Current Trends & Developments*, DATA PROTECTION LEADER, available at http://www.cecileparkmedia.com/data-protection-leader/article_template.asp?Contents=yes&from=dplp&ID=978 [https://perma.cc/9X7Y-SQQC] (last visited Aug. 12, 2018).

56. BUTHE ET AL., *supra* note 35, at 5-6.

57. See also Branislav Hazucha, *Technical Barriers to Trade in Information and Communication Technologies*, in RESEARCH HANDBOOK ON THE WTO AND TECHNICAL BARRIERS TO TRADE 525, 543 (Tracey Epps & Michael J. Trebilcock eds., 2013).

58. BUTHE ET AL., *supra* note 35, at 137.

59. *Id.* at 6.

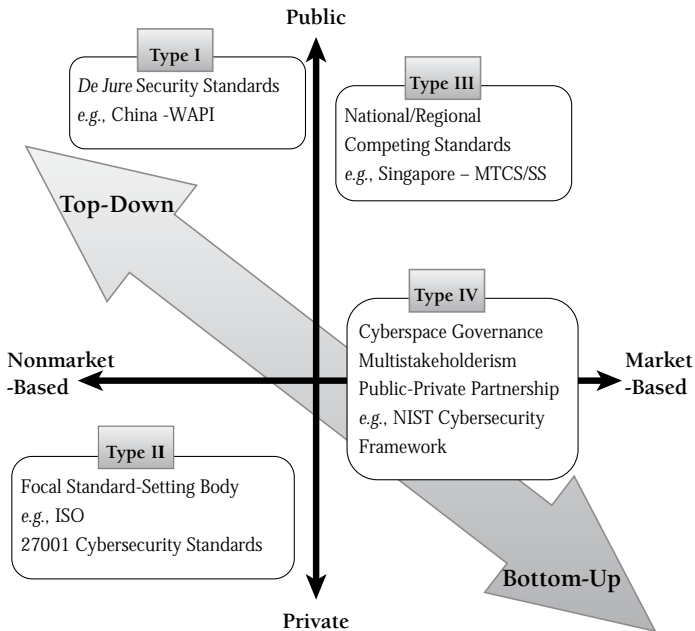
60. SCARFONE ET AL., *supra* note 14, at 1.

61. *Id.*

that an international market for their products will exist.⁶²

At the core of the matter lies this question—how can cybersecurity standards be globally governed? Further, how can a less fragmented and more harmonized cybersecurity regime be established, which would contribute greatly to global economic growth?⁶³ This chapter will distinguish between the four types of cybersecurity standardization,⁶⁴ based on whether the standards are developed in public or private settings (the vertical axis in Figure 1) and whether the standards are created through market competition (the horizontal axis in Figure 1). Placing the “top-down” and “bottom-up” approaches in such a context allows us to identify the features of different types of cybersecurity standard-setting and to recognize the challenges for international economic order.

Figure 1
Harmonization of Cybersecurity Standards: Institutional Setting and Harmonization Mechanism



(Source: Author's analysis and composition)⁶⁵

62. *Id.*; Baisheng An, Institutional Governance for ICT Standards at the International level: Within the WTO and Beyond (unpublished paper based on World Trade Organization thesis (Oct. 2008–Sept. 2009)) (on file with the Cornell International Law Journal).

63. See Peng, *supra* note 20, at 328, 333–35.

64. Buthe & Mattli created a “typology to distinguish modes of global regulation.” The types of standards in this are also based on public/private and market/nonmarket-based regulation. See BUTHE ET AL., *supra* note 35, at 19, 33. See also Walter Mattli, *Beyond the State? Are Transnational Regulatory Institutions Replacing the State?* in THE OXFORD HANDBOOK OF TRANSFORMATIONS OF THE STATE 285, 289–97 (Stephan Leibfried et al. eds., 2015).

65. See *id.* This figure is based off the work of Buthe and Mattli.

A. The “Traditional” Mechanism: A Possible Blind Alley

As shown in <Figure 1>, the ISO standards are established in private international institutions, and this process does not entail market competition (Type II).⁶⁶ These types of standards once played a prominent role in standards harmonization across jurisdictions. Governments have long committed to using the ISO standards as the technical basis for domestic regulation,⁶⁷ through either *ex post* endorsement or *ex ante* delegation of public regulatory authority. In most cases, the legislators or regulators “borrow” ISO standards to incorporate into domestic regulations. At other times, domestic laws simply include a general reference to the specific ISO standard, with the mandate that the regulatory obligation will be automatically transferred to the revised standard if such a standard subsequently changes.⁶⁸

The ISO 27001 on cybersecurity, however, has a relatively low adoption rate worldwide.⁶⁹ In the past, standards of the communications sector have been governed by the so-called big three: the ISO, the International Electrotechnical Commission (“IEC”), and International Telecommunications Union (“ITU”). Today, these traditional organizations are complemented and at times replaced by multiple industry-centered consortia.⁷⁰ The ICT business consortia are reportedly producing cybersecurity standards in a manner that has meant even the ISO 27001 has been challenged, if not outpaced, by new informal standard setters.⁷¹ An empirical analysis has demonstrated that the ISO 27001 standard, when compared to the other ISO standards, has received significantly less interest from the industry as measured by the rate of adoption.⁷² The low adoption rate of the ISO cybersecurity standards, in my view, is primarily attributable to the three following reasons.

First, compared with the emerging market-driven, bottom-up approaches, the ISO requires a relatively long time to develop international consensus on positions. An ISO standard generally takes several years from inception to publication in order to meet the consensus procedural requirement, which—among other elements—includes the use of the ISO

66. *Id.* at 19.

67. See Arcuri, *supra* note 20, at 494. ISO has observer status in the TBT Committee. Reference to the ISO is found in the TBT Agreement. However, whether ISO standards are international standards within the meaning of the TBT Agreement remains disputed.

68. *Id.*

69. The ISO/IEC 27000 is the best-known standard providing requirements for an information security management system (ISMS), which is a systematic approach to managing sensitive company information so that it remains secure and helps organizations keep information assets secure. See ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, available at <https://www.iso.org/isoiec-27001-information-security.html> [<https://perma.cc/578Q-KE4Q>] (last visited Aug. 12, 2018).

70. Pauwelyn, *supra* note 20, at 743.

71. *Id.*

72. Vladislav V. Fomin et al., *ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption*, EURO MOT 2008—THE THIRD EUROPEAN CONFERENCE ON MANAGEMENT OF TECHNOLOGY (2008).

five-step process involving multiple draft reviews, comments from national bodies, an international ballot, and the vote of each national body.⁷³ Considering the nature of cybersecurity, in which public and private sectors attempt to adapt to rapid technological changes, the ISO may fail to address and manage cybersecurity risk in a cost-effective way based on business needs.

In addition, the legitimacy and accountability issues of the ISO have further weakened its function in developing cybersecurity standards.⁷⁴ Unlike other standards areas, cybersecurity standards are by nature socio-technical in the sense that such standards have both human/social and technological elements that are strictly intertwined.⁷⁵ Cybersecurity standardization is therefore far more complex than a purely technical, classical standardization approach.⁷⁶ In the domain of cybersecurity, “multistakeholderism” requires a multi-disciplinary approach that appears difficult to achieve under the ISO regime, which has been labeled a club dominated by certain industrial groups in which civil societies are excluded from decision-making procedures.⁷⁷

Furthermore, it should be emphasized that the ISO is not operationally self-sufficient, and its officials do not work in isolation.⁷⁸ Domestic standards bodies are an important component of the ISO institutional structure, and they seek to promote and defend the regulatory preferences of their stakeholders to minimize domestic switching costs.⁷⁹ In other words, standards should not be seen as norms which embody some objective truth or undisputed scientific wisdom—neither is the ISO process apolitical.⁸⁰

With respect to <Figure 1>, it should also be noted that similar logic can be applied to market-based public standards (Type III, Figure 1).⁸¹

73. INT’L CYBERSECURITY STANDARDIZATION WORKING GRP. OF THE NAT’L SEC. COUNCIL’S CYBER INTERAGENCY POLICY COMM., SUPPLEMENTAL INFO. FOR THE INTERAGENCY REPORT ON STRATEGIC U.S. GOV’T ENGAGEMENT IN INT’L STANDARDIZATION TO ACHIEVE U.S. OBJECTIVES FOR CYBERSECURITY, available at <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf> [<https://perma.cc/5BD9-CKVR>].

74. Arcuri, *supra* note 20, at 495. The ISO has been labeled a club dominated by private industrial groups where developing countries and civil societies are excluded from information and decision-making procedure. The privileged status of ISO raised the controversy on its legitimacy and accountability.

75. See EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *supra* note 37.

76. See *id.*

77. See Arcuri, *supra* note 20, at 495.

78. See BUTHE ET AL., *supra* note 35, at 12.

79. *Id.* See also Hazucha, *supra* note 57, at 533. The losing companies have to bear the cost of developing technical solutions which were not successful in the competition with the adopted standard.

80. See BUTHE ET AL., *supra* note 35, at 12.

81. For example, the Multi-Tier Cloud Security Standard for Singapore (MTCS SS) issued by the Infocomm Development Authority of Singapore (IDA), which aims to provide businesses with greater clarity on the levels of security offered by different cloud service providers (CSPs), is the world’s first cloud security standard. See *Singapore Launches Multi-Tier Cloud Security Standard*, INFOCOMM MEDIA DEVELOPMENT AUTHORITY (Nov. 3, 2017), <https://www.imda.gov.sg/infocomm-and-media-news/whats-trending/>

Given that the political and economic stakes in cybersecurity standard-setting can be enormous, it is difficult, if not impossible, for national or regional standards to win out over other standards as the global standard after a period of public rule-making competition among public regulators.⁸² To conclude, cybersecurity standard-setting is not merely about who commercially wins and who loses. It is also politically sensitive and complex. Reasons, such as conflicting political agendas, national security concerns, and competition for global influence, have created a rather difficult situation in the arena of cybersecurity standards harmonization.⁸³

B. Market-Based “Private” Standard-Setting: The Organically Evolving Norms

1. Cyberspace Governance and Multistakeholderism

As advocated by the ICT industry and relevant civil societies, governments are important components of Internet governance, but they do not play an exclusively dominant role. Through a relatively inclusive and transparent process,⁸⁴ “polycentric partnerships”—from the private sector to civil society to technical experts to governments—represent the constituency of a truly global governance sphere.⁸⁵ In other words, governments, working together with other relevant stakeholders, participate on equal footing as representatives of their respective constituents.⁸⁶ Therefore, this represents a new approach to cybersecurity that seeks out best practices from the public and private sectors by fostering multistakeholder collaboration.⁸⁷

Is it possible to produce bottom-up, market-based outcomes for cybersecurity (Type IV, Figure 1) in a global environment? Indeed, it was this bottom-up “private” mechanism that gave the Internet its momentum and

2013/12/singapore-launches-multitier-cloud-security-standard [https://perma.cc/NNQ7-A2SA] (last visited Aug. 12, 2018).

82. See BUTHE ET AL., *supra* note 35, at 9.

83. See Shackelford et al., *supra* note 20, at 255.

84. Pauwelyn, *supra* note 20, at 739, 748–51.

85. The Internet Governance Forum (IGF), as an example, was formed due to the growing unease with US control over ICANN. Since its inception, IGF seeks to bring together a variety of representatives from academia, civil society, private sector groups, and governments to discuss and shape Internet governance policy. See Vinton G. Cerf et al., *IoT Safety and Security as Shared Responsibility*, 1(35) BUSINESS INFORMATICS 7, 13 (2016).

86. *Id.*

87. The term “multistakeholderism” refers to “two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature.” Mark Raymond & Laura Denardis, *Multistakeholderism: anatomy of an inchoate global institution*, 7:3 INT’L THEORY 572, 573 (2015). In practice, there are various types of multistakeholder governance, produced by variation on the types of actors involved and the nature of authority. See generally William H. Dutton, *Multistakeholder Internet Governance?*, in BACKGROUND PAPER: DIGITAL DIVIDENDS 2–5 (2016); Kal Raustiala, *Governing the Internet* (UCLA Sch. L. Pub. L. & Legal Theory Res. Paper Series, Res. Paper No. 16–33 (2016)); STEFAAN G. VERHULST, *THE PRACTICE AND CRAFT OF MULTISTAKEHOLDER GOVERNANCE: THE CASE OF GLOBAL INTERNET POLICYMAKING* 8–9 (2016); Shackelford et al., *supra* note 20, at 245; CIGI, *supra* note 20, at 2.

enabled the phenomenal level of innovation that has characterized the Internet.⁸⁸ How, then, could such highly flexible, decentralized and polycentric governance arrangements—involving many different institutions and individuals—help to harmonize cybersecurity standards? Examining the history of “traditional standards wars,” it is clear that one firm’s proprietary solution may become the global de facto technical standard if that firm attains a dominant position in the market.⁸⁹ In other words, market competition between competing private standards can be an effective means of moving toward de facto standardization.⁹⁰ Could any Type IV standard-setting entity succeed in establishing its technology as the market-dominant de facto international standard as a result of widespread acceptance in the market? Would such a market-based, public-private international standard-setting mechanism occur in the context of cybersecurity?⁹¹

2. Emerging Norms and the Direction of Evolution

Again, taking the NIST Framework as an example, although “voluntary,” the framework is nonetheless highly influential. Industry is increasingly referencing the framework as a de facto cybersecurity standard.⁹² According to a relevant survey, the framework is now used by approximately 30 percent of U.S. organizations, and this estimate is projected to reach 50 percent by 2020.⁹³ In fact, the framework has already been influential not only in the U.S., but also in other jurisdictions.⁹⁴ Such harmonization is a critical first step toward cyberspace norm development that could, in time, lead to international cybersecurity standards.⁹⁵

As previously discussed, since its creation, the framework serves as a common set of terms and language for discussing cybersecurity within industry and government, which over time helps to harmonize global cybersecurity best practices and shape global standards. Industry use of the NIST Framework of cybersecurity standards is growing throughout Canada, Latin America, Europe, and Asia. In Japan, for example, the framework and ISO 27001 are complementary tools,⁹⁶ and a recent survey revealed that 33 percent of participating organizations referred to the NIST best practices as their cybersecurity standards. It is acceptable to state that

88. See Dutton, *supra* note 87, at 33.

89. See BUTHE ET AL., *supra* note 35, at 14; Arcuri, *supra* note 20, at 521. Examples of de facto standards include Microsoft Windows operating systems and Sony’s Blu-ray format that won over Toshiba’s HD DVD to become a global standard for optical discs.

90. See BUTHE ET AL., *supra* note 35, at 14.

91. *Id.* at 25–32.

92. See, e.g., AMAZON WEB SERVICE, NIST CYBERSECURITY FRAMEWORK (CSF)—ALIGNING TO THE NIST CSF IN THE AWS CLOUD 5 (2017).

93. *Id.*

94. See *id.*

95. Shackelford et al., *supra* note 20, at 254.

96. Charlie Mitchell, *Japanese Industry Leader on Cyber: NIST Framework Increasingly Embraced Overseas*, INSIDE CYBERSECURITY (July 25, 2017), <https://insidecybersecurity.com/daily-news/japanese-industry-leader-cyber-nist-framework-increasingly-embraced-overseas> [<https://perma.cc/Z4MX-7DCY>].

the framework has the potential to become a de facto international cybersecurity standard.⁹⁷

As globalization has created markets that cross borders,⁹⁸ there is an increasing reliance on a diverse array of mechanisms to "harmonize" international affairs.⁹⁹ An international arrangement that is designed as an instrument of global governance can be placed on a continuum from "hard law" to "soft law"¹⁰⁰ to "informal rules."¹⁰¹ As Joost defined it, informal international lawmaking is unique, but it does incorporate the phenomenon of soft law, as it addresses not only informal output but also new informal actors and processes.¹⁰² Multistakeholderism in cyberspace governance, which features both non-traditional actors/processes and non-traditional outputs, demonstrates the increasingly diverse and creative forms of cooperation outside of international law. This ongoing shift to multistakeholder governance, however, raises a host of important questions. How can the WTO be saved from the risk of irrelevance? How can the WTO become a forum for trade disputes concerning "private" cybersecurity standards created through a multistakeholder process? How can governments be held accountable for Type IV regulatory regimes that impose unjustified barriers to trade? The central question, however, is as follows: is the TBT Agreement still relevant?

III. Implications for WTO Law

A. Technical Regulation: Saving the TBT Agreement from Declining Relevance

The last decade has witnessed rapidly growing interest among scholars from different disciplines in cyberspace governance and multistakeholderism, which have emerged around the regulation of the Internet. Surprisingly, though, the impact of such phenomenon on the WTO is a topic that has received relatively little attention in the literature. At the crux of the matter is this: the emerging norms in cyberspace have prompted concerns that the WTO is becoming irrelevant.¹⁰³ The proliferation of private regulation could destroy the enormous benefits we derive from the multilateral trading system. The multistakeholder mechanism in cyberspace governance is widely feared to spell the end of the WTO's mul-

97. See Shackelford et al., *supra* note 20, at 254.

98. See Jean Galbraith & David Zaring, *Soft Law as Foreign Relations Law*, 99 CORNELL L. REV. 735, 745 (2014).

99. *Id.*

100. Andrew T. Guzman & Timothy L. Meyer, *International Soft Law*, 2 J. LEGAL ANALYSIS 171, 173 (2010). See also Gunther F. Handl et al., *A Hard Look at Soft Law*, 82 AM. SOC'Y INT'L L. PROC. 371, 371 (1988). See also Jonathan Carlson, *Hunger, Agricultural Trade Liberalization, and Soft Law: Addressing the Legal Dimensions of a Political Problem*, 70 IOWA L. REV. 1187, 1200-01 (1985).

101. See Pauwelyn, *supra* note 20, at 742; Carlson, *supra* note 100, at 1203.

102. See Pauwelyn, *supra* note 20, at 742.

103. See, e.g., Shawn Donnan, *WTO Wrestles with Relevance in Age of Ecommerce*, FIN. TIMES (Dec. 13, 2017), <https://www.ft.com/content/d9f63c20-e01d-11e7-a8a4-0a1e63a52f9c> [<https://perma.cc/6PNB-GGAP>].

tinational approach, with the WTO gradually moving toward the status of a marginalized talking shop.¹⁰⁴

This Article argues that eventually the WTO panels and the Appellate Body (AB) might have to engage in judicial interpretation of private norms governing cyberspace—in particular, the interpretation of the inevitable clashes between multilateralism and multistakeholderism. In such potential litigation, the complaining party would undoubtedly argue that the measures at issue, i.e., market-based “voluntary” cybersecurity standards developed from “public-private partnership” processes (Type IV, Figure 1), fall under the definition of “technical regulation” in the TBT Agreement.¹⁰⁵ Would such claims regarding the TBT Agreement prevail? Could the panel of the AB strike down an invocation of TBT Article 2.1 given that the “measures,” e.g., the Type IV standards, are not mandatory and therefore are not a “technical regulation” under TBT Article 2.1? It is vital that the complaining members develop arguments to establish that there is sufficient “governmental involvement” under such a public-private “co-governance.”¹⁰⁶ The responding party, on the other hand, may argue that the standards issued by such “transparent and inclusive” processes constitute “relevant international standards” within the meaning of TBT Article 2.4.¹⁰⁷

In short, on the issue of the Type IV cybersecurity standards, the challenges facing the TBT Agreement today are numerous. This section examines four challenges in particular: a challenge to the definition of “technical regulation,”¹⁰⁸ a challenge to the determination of “government action,” a challenge to the distinction of “voluntary/mandatory” compliance,¹⁰⁹ and a challenge to the recognition of the “international standardization bodies” for cybersecurity.¹¹⁰ The fact that a certain Type IV regulation has the

104. See Theodore H. Cohn, *The World Trade Organization and Global Governance, in* NEO-LIBERALISM, STATE POWER AND GLOBAL GOVERNANCE 201, 213 (Simon Lee & Stephen McBride eds., 2007).

105. Agreement on Technical Barriers to Trade, Apr. 15, 1994, 1868 U.N.T.S. 120, 135 [hereinafter TBT Agreement].

106. See ARKADY KUDRYAVTSEV, PRIVATE-SECTOR STANDARDS AS TECHNICAL BARRIERS IN INTERNATIONAL TRADE IN GOODS: IN SEARCH OF WTO DISCIPLINES 159-74 (2005).

107. See TBT Agreement, *supra* note 105, at 121.

108. See *id.* (“Members shall ensure that in respect of technical regulations, products imported from the territory of any Member shall be accorded treatment no less favorable than that accorded to like products of national origin and to like products originating in any other country.”)

109. See *id.* at 135. For the purpose of the TBT Agreement, the following definitions shall apply: “1. Technical regulation—Document which lays down product characteristics or their related processes and production methods, including the applicable administrative provisions, with which *compliance is mandatory.*” *Id.* (emphasis added). “It may also include or deal exclusively with terminology, symbols, packaging, marking or labeling requirements as they apply to a product, process or production method.” *Id.*

110. See *id.* at 121 (“Where technical regulations are required and relevant international standards exist or their completion is imminent, Members shall use them, or the relevant parts of them, as a basis for their technical regulations except when such international standards or relevant parts would be an ineffective or inappropriate means for the fulfillment of the legitimate objectives pursued, for instance because of fundamental climatic or geographical factors or fundamental technological problems.”).

potential to become a de facto cybersecurity international standard has created a renewed sense of urgency for the WTO to take action in order to avoid the fate of being eclipsed into irrelevance in the domain of cyberspace governance. Can the TBT Agreement save the WTO from declining significance in its global governance of the Internet?

B. Government Action: Public, Private, and In-Between

Type IV cybersecurity standardization activities generate many interpretive issues. At the heart of the controversy is the determination of a “government act.” In situations where the adoption, preparation, and application of cybersecurity policy or regulatory schemes are delegated by the government to a private standard entity, or where the “private” standards are incorporated into law—no matter *ex ante* delegation or *ex post* incorporation¹¹¹—it is uncontested that the “private actions” may fall within the scope of the TBT agreement, as a “government endorsement” can be found.¹¹² However, as stressed earlier, the “public-private partnership” in many cybersecurity standardization processes, during which public and private sector actors work together, may fall neither into the public nor the private domain but, rather, “in-between.”¹¹³

The issue of “attribution” of private actions to WTO Members has arisen before the WTO dispute settlement system and was considered by WTO panels and AB in several disputes—in particular, under the rules of the General Agreement on Tariffs and Trade (“GATT”), the Agreement on Subsidies and Countervailing Measures (“SCM”), and the Agreement on Agriculture (“AoA”).¹¹⁴ Considering the approaches taken by the WTO panels and the AB, a Type IV cybersecurity standard may constitute a technical regulation within the meaning of the TBT Agreement if the support provided by a government is sufficient to become a governmental act. In past WTO jurisprudence, private actions could be attributed to governments if there was sufficient governmental involvement.¹¹⁵ In the *US-Corrosion-Resistant Steel Sunset Review* case, the AB stressed that, in principle, any act or omission attributable to a WTO Member can be a measure of that Member for the purposes of dispute settlement proceed-

111. Arcuri, *supra* note 20, at 497.

112. *Id.* See also KUDRYAVTSEV, *supra* note 106, at 238–39.

113. See Kristin E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 470–71 (2017).

114. See KUDRYAVTSEV, *supra* note 106, at 159–74. See also *Panel Reports, European Communities and Its Member States—Tariff Treatment of Certain Information Technology Products*, ¶ 7.1167, WTO Doc. WT/DS375/R/WT/DS376/R/WT/DS377/R, (adopted Aug. 6, 2010).

115. See KUDRYAVTSEV, *supra* note 106, at 159; Arcuri, *supra* note 20, at 498. As Kudryavtsev elaborated in the book, there have been several cases regarding the issue of “attribution” under the WTO jurisprudence, e.g., in the Japan-Semiconductors case. Japan was found to be in violation of Article XI:1 of the GATT as the “voluntary” private export restrictions on the export of semiconductor were attributed to the Japanese government.

ings.¹¹⁶ In *Japan- DRAMs (Korea)*, the panel stated that there must be a demonstrable link between the government and the conduct of the private body.¹¹⁷ Generally speaking, the degree of governmental involvement is decisive for the qualification of a private action as a governmental responsibility. In other words, private conduct will come under the WTO disciplines only if it can be attributed to a WTO member.¹¹⁸

It should be noted, however, that in *Japan- Film*, the AB clarified that neither every utterance by a government official nor every study prepared by a non-governmental body at the request of the government or with some degree of government support can be viewed as a measure by a Member government.¹¹⁹ In other words, WTO panels and the AB do not easily assume the responsibility of Members with regard to private conduct without convincing evidence, and the burden of proof to establish that such a nexus lies with the complainant.¹²⁰ Although the relevant texts themselves do not clarify which measures are to be regarded as those of WTO Members, WTO jurisprudence, as stressed in *U.S.- Gambling*, clarifies that it requires a sufficient “nexus” between government action and private conduct for the attribution of the latter to the former.¹²¹

This Article argues that most of the Type IV standards are controversial in terms of whether such a scheme is delegated by public power. The blurring of public and private and the changing architecture of the state make the identification of “the degree of governmental involvement” a rather complex area. Indeed, public-private schemes are emerging. In the real world, a carrot-and-stick balancing approach might be proven to be the most effective way to promote cybersecurity. Voluntary self-regulation and direct government regulation are mutually exclusive options and fall on the opposing ends of the regulatory spectrum. However, the cybersecurity co-regulatory model, in which public and private sector actors work together, falls somewhere in the middle. One key element of the changing character of cybersecurity is the significance attached to the role of the third party, especially the certification mechanism. The NIST Framework, again serving as an example, demonstrates how a multistakeholder approach could provide a foundation on which to build a certification system as a middle ground between “purely public” and “purely private” cybersecurity certification efforts.¹²²

116. See Appellate Body Report, *United States– Sunset Review of Anti-Dumping Duties on Corrosion Resistant Carbon Steel Flat Products from Japan*, ¶¶ 81–82, WTO Doc. WT/DS244/AB/R (adopted Dec. 14, 2003).

117. See Panel Report, *Japan– Countervailing Duties on Dynamic Random-Access Memories from Korea*, ¶ 7.104, WTO Doc. WT/DS336/R (adopted July 13, 2007).

118. See Mavroidis & Wolfe, *supra* note 21, at 10.

119. See Panel Report, *Japan– Measures Affecting Consumer Photographic Film and Paper* paras. 10.43, 10.45–51, WTO Doc. WT/DS44/R (adopted Apr. 22, 1998).

120. See KUDRYAVTSEV, *supra* note 106.

121. See Appellate Body Report, *United States– Measures Affecting the Cross Border Supply of Gambling and Betting Services*, paras. 121–23, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005).

122. See Shackelford et al., *supra* note 20, at 256.

The emergence of a multiplicity of new actors and different standard-setting bodies therefore results in the question of how international trade agreements will respond to increasing networking between public actors and private participants.¹²³ In the future, WTO panels and the AB might have to face questions as to whether “co-regulation” falls within the scope of the term “technical regulations” in TBT Article 2.1. Can the concept of “technical regulation” be broadly construed in order to cope with the trend of the “privatization of regulation”? Would such an interpretative approach be overbroad and therefore potentially compromise the legal certainty and predictability of the TBT Agreement? Would such an interpretation create the risk that Members will be subject to WTO dispute settlement proceedings even when they did not effectively control or govern the actions of a private body or delegate such responsibility to a private body?

In light of the potential for litigation, it is vital that the complaining party develop arguments to establish that the cybersecurity standards at issue, although arising from a multistakeholder process, involve acts delegated by public powers. There might be a strong argument that, after all, the private sector does not have the powers to oblige third parties to adhere to a certain scheme.¹²⁴ To support this position, the complaining party could draw attention to the fact that the co-regulation mechanism is fulfilling an important role in the cyberspace ecosystem. On the other hand, responding parties might argue that the amount of governmental involvement is decisive for the qualification of private conduct as a governmental responsibility. That said, Type IV standards will come under the WTO disciplines only if they can be attributed to a WTO member.¹²⁵ In this regard, cybersecurity “co-regulation” has shifted the role of government in such a way that it no longer retains general oversight authority to approve and enforce standards.

C. Voluntary/Mandatory Dichotomy: Non-Binding but Compulsory?

The key distinction between technical regulations and standards is that compliance is mandatory with the former and voluntary with the latter.¹²⁶ Under this definition, a Type IV cybersecurity standard may be found to constitute a “technical regulation” within the meaning of the TBT Agreement if the support provided by a government is sufficient so as to render the standard “mandatory de facto.” In *US- Tuna II*,¹²⁷ the Panel at the outset considered the interpretation of the term “mandatory” in Annex 1.1., noted various dictionary definitions, and explained that “mandatory” may encompass the legally binding and enforceable character of the instru-

123. See MARTIN LODGE, *MANAGING REGULATION: REGULATORY ANALYSIS, POLITICS AND POLICY MANAGING* 143 (2012).

124. See KUDRYAVTSEV, *supra* note 106; Arcuri, *supra* note 20, at 498-99.

125. See Mavroidis & Wolfe, *supra* note 21, at 12.

126. See TBT Agreement, *supra* note 105, Annex 1.

127. Panel Report, *United States- Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, paras. 7.102-06, WTO Doc. WT/DS381/R, (adopted Sept. 15, 2011) [hereinafter *US-Tuna II Panel Report*].

ment and may also relate to its contents, prescribing or imposing a certain behavior.¹²⁸ The Panel also stressed that the expression “mandatory requirement” should be used to mean only “a requirement made compulsory by law or regulation.”¹²⁹ A responding party in this hypothetical dispute may counter that the Type IV standards merely constitute “voluntary measures” that are not covered by Annex 1.1.

If the responding party successfully claims that the measures at issue are not technical regulations, it would create a large carve-out under the TBT agreement. At the core of the issue is whether compliance with the Type IV standards is *de facto* mandatory, which would therefore render the measures “technical regulations” under TBT Article 2.1.

In this context, the case of the U.S. Federal Trade Commission (the “FTC”) serves as an interesting example. Since 2000, the FTC has established standards for “cybersecurity due diligence” by bringing dozens of enforcement actions under its general statutory authority—Section 5(a) of the Federal Trade Commission Act—to address “unfair or deceptive acts or practices in or affecting commerce.”¹³⁰ The FTC has brought these actions against companies whose cybersecurity practices it deemed inherently “unfair,” essentially by failing to take appropriate action to assess security risks. In these cases, the FTC consistently establishes *de facto* cybersecurity standards with respect to “reasonable” cybersecurity practices. The reasonableness approach taken by the FTC, however, relies on industry experts to prove unfairness, which is fully compatible with the NIST framework.¹³¹ To illustrate, certain Type IV cybersecurity standards are heavily referred to, if not relied upon, by relevant regulators to the degree that in the real-world compliance with such standards becomes a core requirement for “duty of care.” For example, in 2012, the FTC began proceedings to sue Wyndham Hotels & Resorts LLC, seeking injunctive and other equitable relief for this organization’s “failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information.”¹³² In this particular case, the defendants cited the NIST framework, implying that the framework might represent the regulatory expectation when the FTC brought its enforcement action against Wyndham.¹³³

It is evident that the implementation of the NIST Cybersecurity Framework is emerging as a *de facto* requirement for companies in terms of “cybersecurity due diligence” or “reasonable cybersecurity measures.” It is undeniable that the issues the NIST Framework calls for companies to evaluate are the same issues the FTC has evaluated for years through its Section

128. See Peng, *supra* note 22, at 136.

129. *Id.*; see also US-Tuna II Panel Report, *supra* note 127, para. 7.103.

130. Bruce Heiman et al., *The FTC Has Already Set Cybersecurity Standards*, LAW360 (Mar. 5, 2015), <https://www.law360.com/articles/626447/the-ftc-has-already-set-cybersecurity-standards> [<https://perma.cc/48GN-MHCX>].

131. See Vladimir J. Semendyai, Response, *Due Process and the FTC's Fair and Reasonable Approach to Data Protection*, 84 GEO. WASH. L. REV. ARGUENDO 51, 66 (2016).

132. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 236 (3d Cir. 2015).

133. *Def. Mot. to Dismiss, FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D. N.J. 2014).

5 enforcement when determining whether a company’s data security and processes are reasonable.¹³⁴

Indeed, the FTC’s longstanding Section 5 enforcement takes a similar approach to the NIST Framework.¹³⁵ For example, in the complaints against HTC America, Inc., the FTC alleged that the company did not have a process for receiving, addressing, or monitoring reports about security vulnerabilities.¹³⁶ The framework’s guidance has a similar goal: almost all FTC determinations align with the framework’s guidance that companies should consider having a method for receiving vulnerable information.¹³⁷ The FTC matches its cybersecurity standards with those of the NIST Cybersecurity Framework by ensuring that the framework’s approach is “fully consistent” with the FTC’s approach.¹³⁸ To conclude, existing FTC actions seem to provide a clear standard of care.¹³⁹ The consistency between the FTC’s enforcement and the NIST Framework should signal to companies that the FTC strongly endorses, if not requires, the NIST Framework in the development, supplementation, and maintenance of a data security system. Through long-term practices, the FTC has linked its “reasonableness standard for cybersecurity” to the “voluntary” NIST Framework.

In addition to regulators, judges also frequently resort to Type IV standards to give meaning to concepts in law, specifically when evaluating duty of care in negligence cases.¹⁴⁰ If a company’s cybersecurity practice is ever questioned during litigation or a regulatory investigation, the “standard” for “due diligence,” is highly likely to be the NIST Cybersecurity Framework.¹⁴¹ Such judicial recognition can extend a binding effect to what are otherwise “voluntary” private standards.¹⁴² Of course, the court does not apply Type IV standards as such. Instead, Type IV standards serve as guidelines when it comes to the determination of the required standard of care. Compliance with those standards may not be a sufficient defense, but it does have evidentiary value.¹⁴³ The role of Type IV standards is,

134. NIST’s Cybersecurity Framework is consistent with the process-based approach that the FTC has followed. Put it in another way, FTC has mapped its cybersecurity requirements to NIST Framework. See Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM. (Aug. 31, 2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc> [https://perma.cc/4ZA3-UQP7].

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

139. See generally J. William Binkley, *Fair Notice of Unfair Practices: Due Process in FTC Data Security Enforcement After Wyndham*, 31 BERKELEY TECH. L.J. 1079 (2016); David C. Grossman, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283 (2016); Jeffrey F. Addicott, *Enhancing Cybersecurity in the Private Sector by Means of Civil Liability Lawsuits—The Connie Francis Effect*, 51 U. RICH. L. REV. 857 (2017).

140. See Grossman, *supra* note 139, at 1304-05; Addicott, *supra* note 139, at 892-94.

141. See John Verry, *Why the NIST Cybersecurity Framework Isn’t Really Voluntary*, PIVOT POINT SEC. (Feb. 25, 2014), <https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework/> [https://perma.cc/PEB3-ESZE].

142. *Id.*

143. See BUTHE ET AL., *supra* note 35, at 205.

therefore, becoming central to the establishment of the cybersecurity due diligence requirements,¹⁴⁴ as it is shaping the standard of care for the private sector through private litigation. In any event, the reasonableness standard has a long tradition in many jurisdictions. In the context of cybersecurity, courts may apply the reasonableness standard established under multistakeholderism and rely on expert testimony in litigation. Concerns about legal liability thus become a strong incentive for companies to comply with the Internet norms that are not legally mandated but that define best practice.¹⁴⁵ That said, implementation of the Type IV standards have the potential to emerge as a *de facto* requirement for companies.¹⁴⁶

A common misunderstanding lies in the assumption that non-binding standards are less frequently complied with when compared to mandatory standards.¹⁴⁷ This no longer holds true. Those “private standards” under multistakeholderism may be as constraining, if not more so, as traditional regulations.¹⁴⁸ Compliance with private regulations can be extremely stringent. Regulatory and judicial authorities have played significant roles in reinforcing the rapid privatization of standard-setting.¹⁴⁹

To conclude, private rule-making still takes place in political and legal contexts at the domestic level, which is shaped by governments and courts.¹⁵⁰ Private standardization, by its nature, may not always be fully autonomous.¹⁵¹ To a great extent, the Type IV cybersecurity standards are “non-binding” but somehow “compulsory.”

D. International Standardization Bodies: The Openness Test?

Another interesting aspect is the exploration of whether a WTO member, regardless of its status as a complainant or a respondent, can establish an “international cybersecurity standard” within the meaning of TBT Article 2.4,¹⁵² based on the fact that certain Type IV schemes are highly influential and thus constitute a “relevant international standard” within the meaning of TBT Article 2.4. In *US-Tuna II (Mexico)*, the AB further confirmed that by virtue of Article 2.4, if a standard is found to constitute a “relevant international standard,” WTO Members are required to use it or

144. *Id.* at 205-06.

145. *Id.* at 6.

146. See Shackelford et al., *supra* note 20, at 225-26, 256.

147. See Pauwelyn, *supra* note 20, at 745.

148. *Id.*

149. See BUTHE ET AL., *supra* note 35, at 25.

150. *Id.* at 25.

151. See Pauwelyn, *supra* note 20, at 746, 749.

152. According to Article 2.4, technical regulations that use international standards are presumed, subject to rebuttal, to be consistent with WTO obligations; on the other hand, the use of a standard that differs from the pertinent international standard may be challenged as an unnecessary trade barrier. See TBT Agreement, *supra* note 105, art. 2.4.

its relevant parts, as a basis for their technical regulations.¹⁵³

While the heart of the TBT is the adoption of international standards for the sake of trade liberalization, the TBT does not define the term “international standards” per se. The TBT committee attempted to clarify this question but still found it hard to proceed.¹⁵⁴ The AB in *US- Tuna II* stated that in order to constitute an “international standard,” a standard must be adopted by an “international standardizing body” for the purposes of the TBT Agreement.¹⁵⁵ A “standardizing body” does not need to have standardization as its principal function, or even as one of its principal functions, as long as WTO Members “have reason to expect that the international body in question is engaged in standardization activities.”¹⁵⁶ In other words, such a “body” simply has to be “active in standardization,” and the body’s activities in standardization “must be aware.”¹⁵⁷ At the crux of the issue is whether members should recognize the broader WTO definition of “international standardization bodies or systems” contained in Annex 1 of the TBT. It seems that members would have sufficient room to develop creative arguments regarding whether the Type IV regimes could be “international standardizing bodies” under TBT Article 2.4.¹⁵⁸

One tricky issue here is the key characteristics of multistakeholder governance. The AB in *US- Tuna II* argued that a body is “open” if membership to the body is not restricted, and it is not “open” if membership is a priori limited to the relevant bodies of only some WTO members.¹⁵⁹ On this point, it would be interesting to see how parties develop arguments that the standards issued by such “transparent and inclusive” multistakeholder processes constitute a “relevant international standard” within the meaning of TBT Article 2.4.¹⁶⁰ Unlike the ISO, which has been labeled a club dominated by private industrial groups where developing countries and civil societies are excluded from information and decision-making procedures,¹⁶¹ the actors involved in emerging private cybersecurity platforms are much more diverse, inclusive, and transparent. The norms developed are generally more carefully elaborated and are also supported by a broader consensus.¹⁶² After all, transparency of inputs, process, and decision mak-

153. See Appellate Body Report, *United States—Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, ¶ 348, WTO Doc. WT/DS381/AB/R (adopted May 16, 2012) [hereinafter Appellate Body Report, *US- Tuna II*].

154. See Lu, *supra* note 23, at 46–47. See also Peng, *supra* note 22, at 142.

155. Appellate Body Report, *US-Tuna II*, *supra* note 153, ¶¶ 355–59.

156. *Id.* ¶ 362.

157. *Id.* ¶ 360.

158. If we proceed on the assumption that certain Type IV regulations are relevant international standards within the meaning of Article 2.4., the next question is whether such international standards would be an ineffective or inappropriate means for the fulfillment of the legitimate objectives pursued by any other WTO member. The legitimate objectives in Article 2.4 should be understood in the context of 2.2, as the lists of legitimate objectives in 2.2 can be justifications for deviating from international standards. See also Peng, *supra* note 22, at 142–43.

159. See Appellate Body Report, *US-Tuna II*, *supra* note 153, ¶ 364.

160. See Arcuri, *supra* note 20, at 506.

161. *Id.* at 495, 512.

162. See Pauwelyn, *supra* note 20, at 747–48.

ing is fundamental to the Internet.¹⁶³

Conclusion

The following questions were raised at the outset of this Article: how can the WTO be saved from the risk of irrelevance? How can the WTO become a forum for trade disputes concerning “private, voluntary” cybersecurity standards created through a multistakeholder process? How can governments be held accountable for Type IV regimes in situations in which they impose unjustified barriers to trade? To answer the question as to whether the TBT Agreement is still relevant, four specific challenges are examined: a challenge to the definition of “technical regulation,” a challenge to determination of “government action,” a challenge to the distinction of “voluntary/mandatory” compliance, and a challenge to the recognition of the “international standardization bodies” for cybersecurity.

The business sector has actively taken on the standardization initiative. More and more jurisdictions have been settling on a bottom-up approach to cybersecurity policymaking, which aims to minimize mandatory governmental regulation and to favor a voluntary private-sector standard to enhance cybersecurity. To analyze the privatization of governance in a systematic way, this Article placed the “top-down” and “bottom-up” approaches in such a context that allows us to identify the features of different types of cybersecurity standard-setting and to recognize the challenges to international economic order. Given that the political and economic stakes in cybersecurity standard-setting can be enormous, it is difficult, if not impossible, for national or regional standards to win out over other standards as the global standard after a period of public rule-making competition among public regulators. As a result, at the crux of the matter is whether Type IV standards can become *de facto* international standards due to their broad acceptance in the market. If in fact they can, what are the impacts of such a phenomenon on the WTO?

In conclusion, Type IV standardization activities generate many interpretive issues. At the heart of the controversy lies the determination of a “government act.” The blurring of public and private and the changing architecture of the state render the identification of “the degree of governmental involvement” a rather complex area. The concept of a “technical regulation” should be broadly construed in order to cope with the trend of the “privatization of regulation.” However, if such an interpretative approach becomes overbroad, it may compromise the legal certainty and predictability of the TBT Agreement, creating the risk that Members will be subject to WTO dispute settlement proceedings even when they did not effectively control the standard-setting process. After all, cybersecurity “co-regulation” has shifted the role of government in such a way that it no longer retains general oversight authority to approve and enforce standards. Moreover, this Article stresses that cybersecurity standardization

163. See, e.g., Raustiala, *supra* note 87, at 10.

under multistakeholderism is “non-binding” but also somehow “compulsory.” Regulators and judges frequently resort to private standards to give meaning to concepts in law, more specifically, when evaluating duty of care in negligence cases. The so-called “private, voluntary” standards are shaping the standard of care for the private sector and at the same time are becoming central to the establishment of cybersecurity due diligence requirements.

Finally, cyberspace governance is a complex problem. The fact that certain informal norms have the potential to become *de facto* international standards creates a renewed sense of urgency for the WTO to take action in order to avoid the fate of being eclipsed into irrelevance in the domain of cyberspace governance. Eventually, the WTO panels and the AB might have to engage in judicial interpretation of private norms governing cyberspace, and in particular, the inevitable clashes between multilateralism and multistakeholderism.