DRAFT: Please do not cite or
quote without permission.
April 18, 2019

The Internet of Things Cybersecurity Challenge to Trade and Investment: Trust and Verify?

Joel P. Trachtman[1]

Abstract

This paper describes the problem of cybersecurity-based concerns regarding trade in IoT goods, and investment in manufacturing or distribution facilities for IoT goods, analyzes the applicable international law that would constrain national cybersecurity-based import or investment restrictions, and evaluates the availability of security or other exceptions to permit these defensive measures. Based on the defensive needs, and the legal constraints, it suggests some of the characteristics of a cooperative regulatory regime that can foster international trust or verification to allow trade and foreign investment in relation to IoT goods. Trade and investment in low risk consumer IoT products, such as household objects, will be manageable along traditional lines of other product standards, regulated by existing treaties such as the GATT and TBT Agreement to assure national treatment, MFN treatment, proportionality, and due respect for international standards. With respect to high risk industrial, infrastructural, medical or transportation IoT products, the path to liberal trade and investment is less clear, and will depend on the technical ability to surveil and confirm the safety of IoT products. It will be difficult to rely on trusted suppliers, whether on the basis of nationality or territoriality, because of the complexity of production and the magnitude of risk. States will restrict imports and investment in connection with high risk IoT products under security exceptions in trade and investment law, although the specific language of those exceptions do not necessarily support such restrictions. In some circumstances, restrictions will be based on protectionism or geoeconomic considerations, rather than cybersecurity per se. In order to avoid inefficient restriction, states will find it useful to identify means to verify security of high risk IoT products, as well as to establish trust in producers of high risk IoT products, and on the basis of sufficient combinations of verification and trust, to relax their use of security exceptions.

[1] Professor of International Law, The Fletcher School of Law and Diplomacy, Tufts University. I am grateful to Tomer Broude, Susan Landau, Josh Meltzer, and Scott Shackelford for advice and comments. Remaining errors are mine.

1. Introduction

A useful definition of the internet of things (IoT) is provided by the International Standards Organization (ISO):

> IoT is defined as an infrastructure of interconnected physical entities, systems and information resources together with the intelligent services which can process and react [to] information of both the physical world and the virtual world and can influence activities in the physical world.

At the core of the IoT cybersecurity problem is the very fact that IoT devices are connected devices, and so capable of, and subject to, cyber-intrusion through their connections. The growing importance of IoT goods raises at least three types of concerns: (i) risks of cyberattack through IoT goods, (ii) protectionism in the trade sense effected through restrictions on imports of IoT goods,[2] or foreign investment relating to IoT goods, under cybersecurity pretext, and (iii) geoeconomic/technological competition-motivated protectionism effected through such restrictions. In order to manage these conflicting concerns, without disproportionately impeding trade, it will be necessary for states to establish systems that require adequate security verification as a condition for market access. This paper explores the possible structure of such systems.

The challenges presented by cybersecurity are not wholly novel, but their density, complexity and weight have not been seen before. As (and assuming) society becomes increasingly electronically connected, the density, complexity, and weight of the challenges may be overwhelming. Cybersecurity challenges presented by goods and equipment that are connected to the internet include ensuring that these goods and equipment are sufficiently safe from use in (i) attack on individual or other non-governmental privacy, (ii) disinformation or other less serious attack on system integrity, (iii) less serious physical attack on individuals or property, (iv) espionage against governments, (v) attack on critical infrastructure, or (vi) more serious physical attack on individuals or property.

IoT goods can include consumer goods, ranging from children's toys to medical devices to automobiles, and will become increasingly pervasive as goods are increasingly connected. However, critical trade in goods also includes large-scale equipment such as industrial controllers, network equipment, and all sorts of other infrastructural equipment. In this paper, I will divide IoT into two categories on the basis of magnitude of risk: "low risk IoT" includes devices where the risk of cyberattack—items (i), (ii) and (iii) above—does not ordinarily involve catastrophic consequences, and "high risk IoT" includes devices where cyberattack—items (iv), (v) and (vi) above—could cause catastrophic consequences. Obviously, there are gradations between these categories, and different types of risk, but these categories will serve to simplify discussion.

---

[2] For an analysis focusing on the possibility of protectionism, *see, e.g.* Dan Ikenson, Cybersecurity or Protectionism? Cato Institute Policy Analysis, July 13, 2017, available at https://object.cato.org/sites/cato.org/files/pubs/pdf/pa815.pdf.

Ultimately, it is not for this paper to determine what types of IoT pose what types of risks—this will be the job of national and international regulators. But it is also true that even devices that ordinarily seem benign could band together in a botnet that can take critical systems offline, or be used to infiltrate high risk devices, so that the risk can be greater. This fact will suggest regulatory cybersecurity approaches that recognize this and demand protections in low risk IoT, and that insulate high risk IoT from such infiltration.

Cybersecurity risks arise from the hardware, software and firmware contained in these IoT goods, including updates that are made periodically over the life of the goods as well as the very fact that they are connected and so constantly linked to the network, as well as from vulnerabilities that may result from the design of the hardware itself.

The simple, but draconian, solution is to reject the use of IoT goods, perhaps for items (iv), (v) and (vi), or at least for devices such as industrial equipment or vehicles that may be used as weapons of mass destruction. This seems unattractive only if there is a less restrictive means to provide satisfactory security against the use of IoT goods as weapons of mass destruction. Furthermore, goods with large enough batteries or other components that can be used for destruction, and goods that perform large enough physical functions, can be aggregated to effect mass destruction, so the category of goods capable of use as weapons of mass destruction may be quite large.

One less restrictive means of providing satisfactory security is to restrict the providers of IoT goods to a group of trusted suppliers. One proxy that may be used to identify trusted suppliers is that of location. This proxy obviously is overbroad and underinclusive, yet it may serve for some purposes. It is overbroad insofar as local production cannot ensure security. It is underinclusive because some persons that produce abroad can be trusted. Furthermore, given the complexity of supply chains for components and relevant services, it is not enough to have a trusted supplier: the supplier's suppliers must also be trusted. Indeed, under modern supply chain production, it is often impossible to have efficient production of complex goods without deep supply chains involving suppliers from multiple countries.

Location or nationality may be useful proxies for trustworthinesss for some purposes, especially those where the magnitude of possible damage is smaller. However, location or nationality would be insufficient for other purposes, especially under formal definitions of nationality that might allow a foreign power to control a formally domestic corporation. Additional conditions may support trustworthiness. Even if location or nationality were a satisfactory proxy, its use would raise issues of differential treatment of foreign producers, possibly violating international trade law or international investment law unless a national security or other exception is applicable.

The goal of this paper is to describe the problem of cybersecurity-based concerns regarding trade in IoT goods, and investment in manufacturing or distribution facilities for IoT goods, to assess the pressure that these concerns place on security exceptions in international trade law and international investment law, and to formulate a more nuanced response in terms of a cooperative regulatory regime that can foster international trust or verification to allow trade and foreign investment in relation to IoT goods to continue. Otherwise, states may assert security

exceptions to their trade and investment commitments, blocking trade and investment more broadly than necessary to achieve their security goals. In order to carry out this analysis, this paper is organized as follows.

In Part 2, I explain the problem of trade and investment in IoT goods in more detail, using the example of concerns regarding Huawei network equipment to motivate and illustrate the problem. I distinguish among the types of likely threats posed by different types of IoT goods. Different types and levels of threat will call for different systems for verification. For example, it is unlikely that transponders included in crates of bananas to track their location will pose significant existential threats, but they might threaten privacy.

In Part 3, I review the initiatives developed by private national and international standards organizations and by governments regarding the technical requirements for protecting against cyberattack through IoT goods. This includes means for verification or certification of products. These initiatives are still in their nascent stages, often providing broad guidelines for processes to be followed in developing security standards for particular goods, but as they develop they may encounter constraints under international trade and investment law.

In Part 4, I briefly review the types of existing trade and investment law that may constrain national or even international responses to the threat of cyberattack through IoT goods, as well as the potential application of security exceptions in international trade and investment law. Some security exception clauses allow greater subjective determination by the state asserting the exception of the necessity of trade barriers, while others provide for more of an objective test subject to adjudicative determination.

This review will allow me in Part 5 to propose a conditional security exception that only becomes available for specified goods if those goods are not certified through agreed certification procedures, based either on the trusted character of the producer, a verification process for the product, or, more likely, a combination of both. I propose different approaches for low risk IoT compared to high risk IoT. In connection with this discussion, I discuss the extent to which geoeconomic concerns—concerns regarding competition in technical advancement—are, or should be, included within security exception clauses. These concerns are in part cybersecurity concerns, but they are larger than cybersecurity.

2. Cybersecurity Risks Presented by Trade and Investment in IoT Goods

a. Increasing Connectedness of Goods

Although they raise some similar issues, IoT goods present a somewhat different set of cybersecurity issues compared to computers and telecommunications devices themselves. IoT goods are likely to be more ubiquitous and less transparent, and will often interact with the physical world in ways that computers and telecommunications devices do not. They may gather data from the physical world, and they may act upon the physical world. They may act under the control of non-owners, or may act autonomously or robotically. The connectedness of goods is

increasing rapidly. Consider the following large categories of IoT goods, based on a list prepared by the U.S. National Institute of Standards and Technology (NIST):[3]

- Connected vehicles, including drones.
- Consumer IoT including household devices, toys, and other equipment.
- Health IoT devices including data-gathering devices as well as therapeutic devices.
- Smart building IoT.
- Smart manufacturing IoT.

b. Cybersecurity Risks of Low Risk IoT

Different types of IoT goods present different types of risks. A child's toy or a smart speaker may threaten privacy, and could serve as points of entry into other networks, or as bases for botnet attacks on other systems, but would ordinarily not threaten physical harm to the user, or destruction of critical infrastructure. To be clear, not all consumer IoT qualifies as low risk IoT. For example, self-driving automobiles and implanted insulin delivery systems could be used as weapons of mass destruction.

c. Cybersecurity Risks of High Risk IoT

The security risks from high risk IoT goods are, by definition, greater than those for low risk IoT goods. Exploding factories, berserk tractor-trailers, uncontrolled nuclear reactors, crashing airplanes, incapacitated telecommunications or power systems, and unimpeded espionage, are just a taste of the list of unacceptable outcomes. Self-destroying centrifuges, due to hacked controllers, were used in 2009 to impede Iran's nuclear weapons program in the Stuxnet attack.[4]

Recently, an international dispute has arisen regarding the use of Huawei equipment in 5G (5th generation wireless data) networks. While 5G is not itself an IoT application, its greater speed will facilitate the expansion of IoT. More saliently, the risks that 5G networks present are comparable to, and inextricably related to, those presented by high risk IoT. The 5G networks, of course will themselves be critical infrastructure, and will support government, military, financial, and transport sectors—everything. In this sense, they operate at a broader level than individual IoT devices, and constitute a broader threat.

The U.S. has rejected, and sought to persuade other states to reject, Huawei 5G equipment, on the ground that it would expose those other states to cyberattack in the form of espionage or threats to critical infrastructure. Inability to trust 5G networks would also pose risks for smart

---

[3] U.S. National Institute of Standards and Technology, Interagency International Cybersecurity Standardization Working Group, NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), November 2018 (hereinafter "NISTIR 8200"), at v, available at NISTIR 8200.

[4] *See* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014).

factories and all sorts of other IoT uses.[5] Furthermore, the U.S. has stated that it would not be willing to share sensitive security information with states that accept Huawei network equipment, on the ground that this sensitive security information would be rendered insecure by transmission through a Huawei-based network.[6]

China has argued at the WTO that Australia's 2018 restrictions on imports of Huawei 5G technology are discriminatory, raising the question of whether China will bring a case, and whether Australia will defend on the basis of a national security exception.[7] I discuss in Part 4 the WTO law ramifications of import restrictions.

Debates regarding the cybersecurity dimension of Huawei network products have continued for a number of years.[8] In November 2010, the United Kingdom (UK) government negotiated with Huawei the establishment of the Huawei Cyber Security Evaluation Centre (HCSEC) "under a set of arrangements between Huawei and HMG to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure."[9] Huawei has proposed similar arrangements to other countries.[10]

HCSEC is essentially a jointly-established independent undertaking between Huawei and the British government to evaluate the safety of software, and then confirm that the evaluated software matches that actually installed in Huawei equipment. HCSEC is supervised by an Oversight Board led by British intelligence and cybersecurity officials. The remit of the Oversight Board is to review:

- first, HCSEC's assessment of Huawei's products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk which is determined at the NCSC's sole and absolute discretion; and

---

[5] *See* Alex Webb, We Need to Talk About Huawei's Smart Factory Risk, Washington Post, January 9, 2019, available at https://www.washingtonpost.com/business/we-need-to-talk-about-huaweis-smart-factory-risk/2019/01/09/a98e3a6a-13d4-11e9-ab79-30cd4f7926f2_story.html?utm_term=.b5189e9e3349.

[6] Reuters News, U.S. Won't Partner with Countries that Use Huawei Systems: Pompeo, February 21, 2019, available at https://www.reuters.com/article/us-huawei-tech-usa-pompeo/us-wont-partner-with-countries-that-use-huawei-systems-pompeo-idUSKCN1QA1O6.

[7] *See* Reuters News, China Warns Australia at WTO About 5G Restriction, April 12, 2019, available at https://www.reuters.com/article/us-huawei-australia-china-wto/china-warns-australia-at-wto-about-5g-restriction-idUSKCN1RO20H.

[8] *See, e.g.,* US House of Representatives, the House Permanent Select Committee on Intelligence (HPSCI), 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE', 112th Congress, 8 October 2012, available at http://republicansintelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

[9] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018, July 2018, (2018 HCSEC Report), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

[10] Colin Lecher, Can We Trust Huawei With 5G?, The Verge, February 7, 2019, available at https://www.theverge.com/2019/2/7/18214166/huawei-security-china-fcc-5g-cybersecurity.

- second, the independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.[11]

The HCSEC Oversight Board is required to provide an annual report to the UK government regarding the independence, competence and effectiveness of HCSEC. The UK government then makes decisions regarding use of relevant Huawei equipment.

This may be a plausible model for assurance of cybersecurity in network equipment, and also in IoT. It seems designed to supervise and validate both the competence and the independence of the evaluating agency. The essential technical step is to compare the evaluated software with actually installed software. Interestingly, in the case of higher-priced network equipment, it seems possible to check the comparison for each item installed. In its report for the 2017 year, the Oversight Board found a "failure of Huawei R&D to repeatably build a product to a consistent binary." "As described in the previous Oversight Board report, this means that any assurance provided by the overall risk management strategy, and therefore the Oversight Board, is currently limited." The Board noted that "it is the NCSC [UK's National Cyber Security Centre] intent that all products deployed in the UK will have repeatable builds and that HCSEC will be able to routinely show equivalence between the binary installed in UK networks and the binary that can be built from the source code held by HCSEC."[12]

In its March 2019 report for the 2018 year, the Oversight Board concluded that it could "only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term."[13]

This story of careful management of the risk of security threats in telecommunications equipment, and continued inability to assure security, must be read against Chinese policy to require formally private national companies, like Huawei, to support intelligence-gathering. Article 7 of China's 2017 National Intelligence Law requires Chinese companies and citizens to support, assist, and cooperate with state intelligence work according to law."[14] Thus, the fact that a company is nominally or actually private does not provide assurance that it will not participate in cybersecurity threats.

Furthermore, it is necessary to maintain a secure chain of custody from the time that the comparison is carried out to the time when it is installed in a secure facility. In addition, and even more difficult, all software requires updating, if, for no other reason, than to address subsequently identified security flaws. In order to maintain security, it will be necessary to

---

[11] 2008*Id.*, 2018 HCSEC Report, *supra* note 9 at 8, Appendix A.

[12] *Id.*, at 15.

[13] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019, March 2019, at 4, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[14] Murray Scott Tanner, Beijing's New National Intelligence Law: From Defense to Offense, Lawfare, July 20, 2017, available at https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

evaluate the updates for security. Furthermore, the fact that IoT devices are connected to the internet is what makes them most vulnerable. Their connections and software must be designed so that they are protected from hacking.

Assessing a stricter approach that would focus on perceptions of the trustworthiness of suppliers, and their home country governments, rather than attempt to evaluate specific items, the U.S. government is reported to be considering issuing an executive order to declare a national emergency and pursuant to existing statutory authority bar U.S. companies from using telecommunications equipment made by Huawei and ZTE.[15] In addition, the U.S. has already by statute banned federal government purchases of Huawei network equipment. Section 889 of the 2019 National Defense Authorization Act prohibits the use of federal funds to acquire "covered telecommunications equipment or services" which term includes, *inter alia*, certain telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation or their affiliates.[16]

Finally, on February 21, 2019, U.S. Secretary of State Pompeo stated that "if a country adopts [Huawei technology] and puts it in some of their critical information systems, we won't be able to share information with them, we won't be able to work alongside them. In some cases, there's risk we won't even be able to co-locate American resources, an American embassy or an American military outpost."[17]

The U.S. action is alleged by some to be partially influenced by a geoeconomic[18] goal to deny technological supremacy to China in a long-term security competition.[19] "[T]he potential of 5G has created a zero-sum calculus in the Trump White House — a conviction that there must be a

---

[15] David Shepardson and Diane Bartz, White House mulls new year executive order to bar Huawei, ZTE purchases, Reuters, December 27, 2018, available at https://www.reuters.com/article/us-usa-china-huawei-tech-exclusive/exclusive-white-house-considers-new-year-executive-order-to-bar-huawei-zte-purchases-idUSKCN1OQ09P.

[16] The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (H.R. 5515) was signed into law by President Trump on August 13, 2018. This statute has been challenged as an unconstitutional bill of attainder. *See* Wilson C. Freeman, Huawei v. United States: The Bill of Attainder Clause and Huawei's Lawsuit Against the United States, Congressional Research Service, March 14, 2019, available at https://fas.org/sgp/crs/misc/LSB10274.pdf.

[17] Interview with Maria Bartiromo of Mornings with Maria on Fox Business Network, February 21, 2019, available at https://www.state.gov/secretary/remarks/2019/02/289569.htm.

[18] On "geoeconomics," *see* ROBERT D. BLACKWILL & JENNIFER M. HARRIS, WAR BY OTHER MEANS (2017); Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, *Geoeconomics: The Variable Relationship Between Trade and Security*, LAWFARE, Nov. 27, 2018, https://www.lawfareblog.com/geoeconomics-variable-relationship-between-economics-and-security.

[19] David E. Sanger, Julian E. Barnes, Raymond Zhong and Marc Santora, In 5G Race With China, U.S. Pushes Allies to Fight Huawei, New York Times, January 26, 2019: "Mr. Trump's views, combined with a lack of hard evidence implicating Huawei in any espionage, have prompted some countries to question whether America's campaign is really about national security or if it is aimed at preventing China from gaining a competitive edge." *See also* John S. McCain Nat'l Def. Auth. Act for FY 2019, § 1261(a), Pub. L. No. 115-232, Aug 13, 2018, 132 Stat. 1638, regarding a "long-term strategic competition with China."

single winner in this arms race, and the loser must be banished."[20] If this were a strong enough motivation, it would prevent any moderation of the U.S. rejection of Huawei products, both directly for the U.S. and for U.S. allies through persuasion and threat of boycott.

But it is possible that this is not a strong enough motivation, perhaps because the costs of import controls are so high, because allies will not sufficiently join in the collective boycott, or because the disclosure necessary to foster trust in the safety of equipment would also to some degree make it possible to maintain national technological parity. This paper cannot weigh these parameters, so it will proceed to examine how trade in IoT goods can be retained, conditional upon systems for verifying their safety.

Huawei has also been the subject of concern in the field of investment in the U.S., for security reasons. In 2007 and 2008, Huawei sought, partnering with U.S. investment firm Bain Capital, to purchase 3Com, which has since been acquired by Hewlett Packard. However, concerns were raised in the U.S. Committee on Foreign Investment in the United States (CFIUS), because 3Com produced anti-hacking computer software for the U.S. military, among other things.[21]

3. Standards and Technical Regulations to Ensure Safety

The U.S. NIST has proposed that the security objectives that it specifies for industrial control systems can be adapted to IoT systems in general.[22] These security objectives include (i) restricting electronic and physical access to the network, including through firewalls, (ii) protecting individual components from unauthorized access and exploitation, (iii) preventing unauthorized modification of data, (iv) detecting and reporting security events, and (v) maintaining the robustness of networks and components. These types of objectives are elaborated in private and public standards, and are beginning to be elaborated in legal rules as well.

a. Variation by Type of Good or Type of Risk

Risk is a function of the likelihood of the adverse event, interacting with the magnitude of harm upon the occurrence of an adverse event. In the case of some types of low risk IoT, the magnitude of harm upon the occurrence of most imaginable adverse events is relatively low, largely confined to breach of privacy or loss of functionality. It is also true that low risk IoT devices may be used as a weak point of entry into other systems: this can be addressed in security standards for low risk IoT, or security standards for the other systems. By contrast, in the case of transportation IoT, medical devices, and other high risk IoT, for example, the risk may be very high, and any non-zero likelihood of the adverse event may be unacceptable. For purposes of this analysis, I will simplify by focusing on two types of goods: (i) low risk IoT devices, and (ii) high risk IoT devices.[23]

---

[20] *Id.*

[21] Steven Weisman, *Sale of 3Com to Huawei Derailed by U.S. Security Concerns*, New York Times, February 21, 2018.

[22] NISTIR 8200, *supra* note 3, at 25.

[23] I recognize that there will be gradations in between these categories.

The main difference is that for high risk IoT devices, the magnitude of harm upon the occurrence of an adverse event is unacceptable, whereas for low risk IoT devices, it is acceptable. Therefore, the types of safety measures called for differ significantly between the two categories. Low risk IoT devices in this sense are comparable to food, medicines, or other low risk electronic devices: there are significant risks, but safety measures need not totally exclude the risk. Furthermore, because of the more manageable level of risk, low risk IoT devices are less attractive as a military target, and so potential attackers are likely to invest less in mounting an attack.

However, it should be noted that low risk IoT devices, including cell phones, smart watches, and children's toys, present significant security issues, including risks of use in intelligence-gathering through spying on individuals, or through use of big data to reveal troop deployments or other sensitive information. This leads to the question whether restrictions on imports or related investments in connection with low risk IoT devices, or at least certain types of them, might be eligible for application of security exceptions in trade or investment law. I address the scope of these security exceptions in Part 4.

b. Securing Low Risk IoT

As explained above, for low risk IoT devices, perfect security is not necessary. However, good security that reduces the risk of attack will be costly, and is not yet implemented. Due to information asymmetry or collective action problems, it does not appear that consumers yet demand, or that producers yet supply, sufficient levels of security in low risk IoT products.[24]

i. Voluntary Standard-Setting

Voluntary standards are set by non-governmental organizations, but can also be set by governmental organizations. By "voluntary," I mean that the addressee is not formally obliged to comply: it is not command and control regulation. As Bradner and Shackelford have pointed out, "the U.S. has favored a generally voluntary, sector-specific or topic-specific approach to both cybersecurity and data privacy, unlike the more mandatory and comprehensive approach favored in the European Union."[25]

But note that even where the U.S. government does not regulate to *require* action, its recommendations can serve as the standard of care in tort litigation.[26] This mechanism can have greater effects on U.S. persons, subject to the full sweep of U.S. liability rules, than on foreign persons. Interestingly, where this inducement may be weaker for foreign persons, there may be a greater incentive to either treat foreign persons, or certain foreign persons, differently, or to exclude them from the market. Furthermore, tort litigation has a somewhat different temporal effect compared to command and control regulation. Firms that might be judgment-proof,

---

[24] Bruce Schneier, We Need Stronger Cybersecurity Laws for the Internet of Things, November 9, 2018, available at https://www.schneier.com/essays/archives/2018/11/we_need_stronger_cyb.html.

[25] Scott Bradner and Scott Shackelford, Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything, working paper dated January 24, 2009 (on file with the author).

[26] *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

because they have no reachable assets, or firms that are acting intentionally for political or military reasons, may not have adequate incentives to take care to address risk. On the other hand, command and control regulation that is adequately enforced ex ante through surveillance, or for imported goods at the border, may be more effective.

The leading international standard-setting body, the International Organization for Standardization (IOS) has promulgated an IoT-specific "reference architecture" (as discussed below, not an international standard under WTO law). It is descriptive, rather than normative, cataloging generic parts of a system "as a starting point which can be used to create a system specific architecture." It includes issues such as robustness, reliability, and resilience, as well as the following security issues: confidentiality, data integrity, safety, and protection of personally identifiable information.[27]

The U.S. private standard-setting body, Underwriters Laboratories (UL), developed "UL 2900 standards [to] provide manufacturers with testable and measurable criteria to assess software vulnerabilities, weaknesses, and the presence of applicable security controls in the design, development and maintenance of network-connectable products."[28] UL 2900 has been approved by the American National Standards Institute (ANSI), and relevant portions have been adopted by the U.S. Food and Drug Administration as "recognized consensus standards."[29] UL 2900 contains the following components:

1) Requirements regarding the software developer (vendor or other supply chain member) risk management process for their product.
2) Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware.
3) Requirements regarding the presence of security risk controls in the architecture and design of a product.

The Cellular Telecommunications Industry Association (CTIA), a trade association representing the wireless communications industry in the U.S., introduced a cybersecurity certification program for cellular-connected IoT devices in 2018.[30] It involves testing by an independent authorized lab, reporting on the results of tests designed to evaluate the following parameters:

1) Password Management: Device supports local password management

---

[27] ISO/IEC 30141:2018, Internet of Things (IoT) Reference Architecture, August 2018, available at https://www.iso.org/standard/65695.html.

[28] Underwriters Laboratories, Secure Connected Systems and Devices in Consumer IoT Systems, https://ctech.ul.com/en/services/cybersecurity/, visited March 14, 2019. UL offers a separate vehicle cybersecurity program.

[29] Underwriters Laboratories, FDA Recognizes UL 2900-1 Cybersecurity Standard for Medical Devices, September 12, 2017, available at https://news.ul.com/news/fda-recognizes-ul-2900-1-cybersecurity-standard-medical-devices.

[30] Cellular Telecommunications Industry Association, Wireless Industry Announces New Cybersecurity Certification Program for Cellular-Connected IoT Devices, August 21, 2018, available at https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program.

2) Authentication: Device supports user authentication
3) Access Controls: Device enforces role-based access control
4) Patch Management: Device supports automatic and manual installation of patches from an authorized source
5) Software Upgrades: Device supports manual installation software upgrades from an authorized source
6) Audit Log: Device supports the gathering of audit log events and reporting them to an EMS using IPsec, SSH, TLS, or DTLS for encryption and integrity protection
7) Encryption of Data in Transit: Device supports encrypted communications using IPsec, SSH, TLS, or DTLS
8) Multi-Factor Authentication: Device supports multiple authentication factors
9) Remote Deactivation: Device can be remotely deactivated by the EMS
10) Secure Boot: Device supports a secure boot process to protect its hardware
11) Threat Monitoring: Device supports logging of anomalous or malicious activity based on configured policies and rules
12) IoT Device Identity: Device provides an IoT Device Type and a globally unique IoT Device Identity
13) Encryption of Data at Rest: Device supports an effective mechanism for encrypting data stored on the device
14) Digital Signature Generation and Validation: Device supports generation and validation of digital signatures
15) Tamper Evidence: Device has the ability to alert a monitoring system when it is physically opened
16) Design-In Features: Device includes features to fail secure, provide boundary security, and ensure function isolation

In early 2019, NIST issued a discussion draft on Considerations for a Core IoT Cybersecurity Capabilities Baseline, by which it "seeks to identify and propose a minimum set of cybersecurity capabilities (as opposed to controls) for IoT devices."[31] This also does not appear to contemplate a formal regulatory product. It lists 12 candidate capabilities, as follows:

1) The IoT device can be identified both logically and physically.
2) Software and firmware can be updated using a secure, controlled, and configurable mechanism.
3) Authorized users can securely change the IoT device's configuration, and unauthorized changes can be prevented.
4) Local and remote access can be controlled.
5) Can use cryptography to secure stored and transmitted data.
6) Can use industry-accepted standardized protocols for transmissions.
7) Can log cybersecurity events and make them accessible to authorized users.
8) Can be reset by authorized users so all data is securely removed from all internet data storage.

[31] National Institute of Standards and Technology, Considerations for a Core IoT Cybersecurity Capabilities Baseline (Draft), February 1, 2019, at 2, available at https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf.

9) Confirmation of software, firmware, hardware and services is disclosed and accessible.
10) Inventory of software and firmware, including versions and patch status, is disclosed and accessible.
11) Can enforce the principle of least functionality[32] through its design and configuration.
12) Designed to allow physical access to it to be controlled.

In 2018, the U.K. Department of Culture, Media and Sport, working together with the NCSC, published a non-binding "guidance" elaborating a Code of Practice for Consumer IoT Security.[33] It contains 13 guidelines:

1) No default password.
2) Implement a vulnerability disclosure policy.
3) Keep software updated.
4) Securely store credentials and security-sensitive data.
5) Communicate securely.
6) Minimize exposed attack surfaces.
7) Ensure software integrity.
8) Ensure that personal data is protected.
9) Make systems resilient to outages.
10) Monitor system telemetry data.
11) Make it easy for consumers to delete personal data.
12) Make installation and maintenance of devices easy.
13) Validate input data.

To summarize on standard-setting for low risk IoT, there seems to be a developing consensus on the types of security capabilities that low risk IoT devices should have. Specific means for achieving those capabilities, and more importantly, specific measures of the scope of those capabilities, have not been specified. Specific measures of the scope of capabilities may be developed through further legislation, or perhaps in countries like the U.S., through practice or tort litigation. It is likely that the scope of capabilities will be sensitive to the context: greater capabilities will be needed for self-driving cars than for refrigerators that report on grocery needs. These initiatives suggest that, although context and risk are critical determinants, perfect security is not necessary.

ii. Governmental Technical Regulations

[32] Distributing information and resources to modules within the system on a "need to know" basis.
[33] U.K. Department for Digital, Culture, Media, and Sport, Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home, 28 February 2019, available at https://www.gov.uk/government/collections/secure-by-design. *See* Tom Reeve, "Government could regulate IoT security as it launches industry code of practice," SC Media, October 15, 2018.

Manufacturers have been slow to secure low risk IoT devices, and despite the possibility of tort liability, there are externality, information asymmetry, and time inconsistency reasons why government action may be required.

Because it is costly and cumbersome to design different IoT products for different markets,[34] (i) there will be a strong tendency to move toward the highest standard demanded by any regulator, and (ii) providers will seek to ensure that standards are compatible enough that they do not need to design separate software and hardware for separate markets. This might be called a "California effect" or a "Brussels effect," and it suggests that there are some incentives for states, and their native suppliers, to be first mover in this context.

However, there is at the time of this writing very little IoT-specific law in the form of technical regulations. Many countries have privacy laws, and, for example, the European Union General Data Protection Regulation (GDPR)[35] imposes important requirements on IoT. These requirements focus on ensuring privacy of consumer data, including the right to be forgotten. However, this is only one facet of cybersecurity.

At the date of this writing, the U.S. does not have specific regulation for IoT, although of course privacy and other laws are applicable. Thus, similar to the EU, the U.S. does not regulate IoT specifically to reduce risks to consumers or to critical infrastructure. Indeed, at the federal level, Senators Mark Warner, Cory Gardner, Maggie Hassan, and Steve Daines introduced *The Internet of Things Cybersecurity Improvement Act of 2019* (the IoT Improvement Act of 2019) in order to protect government users from risk. The IoT Improvement Act of 2019, if passed into law, would require NIST to issue recommendations on IoT security, and require IoT devices purchased by the U.S. federal government to comply with those regulations.[36]

At the state level in the U.S., California has begun to act, but in a very general, and limited, fashion, focusing on privacy.[37] While the law, effective in 2020, requires "reasonable security features," *inter alia*, "designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure," it is deemed satisfied if each

---

[34] Bruce Schneier, We Need Stronger Cybersecurity Laws for the Internet of Things, CNN Opinion, November 10, 2018, available at https://www.cnn.com/2018/11/09/opinions/cybersecurity-laws-internet-of-things-schneier/index.html.

[35] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018, available at https://gdpr-info.eu/.

[36] Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines, Internet of Things Cybersecurity Improvements Act of 2017, Fact Sheet, available at https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf. Mark R. Warner, Press Release: Bipartisan Legislation to Improve Cybersecurity of Internet-of-Things Devices Introduced in Senate & House, March 13, 2019, available at https://www.warner.senate.gov/public/index.cfm/2019/3/bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-devices-introduced-in-senate-house.

[37] Senate Bill No. 327, An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy, September 28, 2018, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

device has a unique password or requires the user to generate a new means of authentication when it is first used.

c. Securing High risk IoT

Since the main difference between low risk IoT and high risk IoT as I have defined them lies in the greater magnitude of harm that can be incurred through an attack on high risk IoT, the security analysis of high risk IoT is simply an extension, based on an assumption of greater harm, of the security analysis of low risk IoT. The frameworks and standards discussed in connection with low risk IoT above would be relevant to decision-making regarding high risk IoT.

The NIST has begun work on national standards for cybersecurity in what we have termed high risk IoT. In 2014, NIST developed a "Framework for Improving Critical Infrastructure Cybersecurity" (the NIST Framework), which has been revised through April 16, 2018 (NIST Framework 1.1).[38] The NIST Framework was developed to improve cybersecurity risk management in critical infrastructure, but the NIST has suggested that it can also be valuable in assessing risk in other cybersecurity fields.[39] It has also suggested that it "can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities."[40] The NIST Framework is more a checklist or process than a prescription, organized around five core functions relevant to cybersecurity risks: identification of risk, protection against harm, detection of intrusion, response to intrusion, and recovery from intrusion. For example, the NIST Framework 1.1 would provide a process for decision-making regarding cybersecurity in connection with high risk IoT.

The European Union Agency for Network and Information Security (ENISA) has developed "Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures."[41] This comprehensive document is intended to "provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems."[42] Security features recommended include, among others, (i) hardware security features, (ii) integrity management of software, including internet updates, (iii) strong default privacy and security, (iv) protection of privacy, and (v) minimization of risk of physical injury.

---

[38] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 16, 2018) [NIST Framework 1.1], available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[39] *Id.* at v.

[40] *Id.* at vi. *See also* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 Tex. J. Int'l L. 287 (2015); Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Public and Private Sectors,* 17 Chi. J. Int'l L. 1 (2016).

[41] ENISA, Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures, November 2017, available at https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[42] *Id.* at 7.

Of course, the extension of caution in the case of high risk IoT has decisive qualitative implications. Because the amount of harm that can be caused is potentially very great, (i) defending states are unwilling to absorb any significant risk, and (ii) attackers may invest very great resources into preparing an attack, increasing the likelihood of success, and perhaps of attack. For this reason, states would be expected to take much greater precautions to prevent successful attack in connection with high risk IoT.

Thus, high risk IoT goods must be vetted more carefully than low risk IoT goods, and it may be that some states decide that their vetting process can never be preventive enough to ensure against successful attack. As noted at the beginning of this paper in connection with the U.S. approach to 5G networks, one response is to prohibit imports of high risk IoT goods, and to prohibit foreign investment in high risk IoT goods manufacturing. This is an extraordinarily costly response, because it in effect reduces the ability of the protecting state to succeed in an IoT-based economy. Indeed, it would consign the state that took this action to reduced economic welfare, and reduced technological capacity. For this reason, it is at least somewhat self-defeating from a geoeconomic standpoint. It is a dilemma: accept foreign produced high risk IoT goods with the risk they entail, or accept industrial decline with the inevitable security decline it entails.

For some, the very characteristic that defines IoT—connection to the internet—results in inevitable, and in the case of many applications of high risk IoT, unacceptable, risk of hacking or other attack. This position would result in total rejection of IoT for those applications, regardless of the manufacturer. Furthermore, as indicated by the discussion below, it would not raise significant legal issues under international trade or investment law.

Assuming a state decided not to take the total rejection route, it could construct a high risk IoT policy from several components. Assuming that there are externalities, information problems, public goods effects, or other reasons why private entities would fail to take appropriate precautions, the state could insert itself in the high risk IoT security process.

First, it could regulate the design and manufacturing process and ensure sufficient precaution for each application. This would be a regulatory approach that would require the establishment of some parameters for action, and these parameters would inevitably take on the characteristics of technical regulations under the WTO Technical Barriers to Trade (TBT) Agreement, discussed in Part 4.

Second, the state could prohibit use of high risk IoT devices produced by certain untrusted manufacturers. This policy would reflect an admission that application of parameters alone is insufficient, but must be supplemented by a certain degree of trust. The basis for trust might be nationality, location (territoriality), or some different parameters applied to the person rather than to the device. For example, it might be decided to trust a privately-owned firm, but not a state-owned enterprise, or more refined bases for trust might be applied. Furthermore, the state could distinguish between government procurement and private procurement, and limit its prohibition to government procurement (as the U.S. has done in the 5G context,[43] and as the IoT

[43] *See* text accompanying note 16, *supra*.

Improvement Act of 2019 proposes to do). This presumes that cyberattack on government networks is more dangerous than attack on private networks.

Third, the state could prohibit foreign investment in relevant manufacturing and service facilities. This is another type of distinction on the basis of nationality. The U.S. has recently revised its foreign investment review law under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) to extend the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) to transactions involving non-controlling investments in critical technology companies and critical infrastructure companies.[44]

CFIUS is an interagency group within the U.S. federal government, accorded authority to review certain foreign investments to determine whether they threaten to impair US national security. Under amendments to CFIUS' statutory authority made FIRRMA, the scope of threats Congress directed CFIUS to consider included the following:

- How the control of U.S. industries and commercial activity affects the capability and capacity of the United States to meet the requirements of national security, including the reduction in employment of United States persons whose skills are critical to national security and the continued U.S. production of items necessary for national security; and
- Whether a transaction exacerbates cybersecurity vulnerabilities or allows a foreign government to gain new capabilities to engage in malicious cyber activities against the U.S., including activities designed to affect the outcome of any federal election.

This will likely result in a number of transactions relating to investment in IoT production or infrastructure to be blocked for security reasons. "CFIUS seems to have become a major hurdle to Chinese acquisitions of U.S. technology."[45]

4. Trade and Investment Law Restrictions on IoT Cyber-Defense

The types of measures discussed above raise a broad range of international economic law issues. I will focus on issues under WTO law and under bilateral investment treaties. WTO law contains requirements for states to reduce barriers to market access for goods (the *General Agreement on Tariffs and Trade* or GATT) and, to a more limited extent, services (the *General Agreement on Trade in Services* or GATS). The obligations under GATT with respect to product standards and technical regulations are elaborated further in the *Agreement on Technical Barriers to Trade* (TBT). Finally, the WTO includes a plurilateral *Agreement on Government Procurement*, amended as of 30 March, 2012 (GPA), to which 19 members, plus the 28 European Union (EU) members, adhere.[46]

This section will examine the WTO law restrictions contained in the GATT, TBT, GATS, and GPA, as well as restrictions under bilateral investment treaties. I do not separately consider regional or plurilateral integration agreements, such as the North American Free Trade

---

[44] Foreign Investment Risk Review Modernization Act of 2018, H. R. 5515—539 (2018).

[45] Ikenson, *supra* note 2.

[46] China is not a party, but as of March 10, 2019, was listed on the WTO website as negotiating accession.

Agreement or the European Union. These agreements (other than the European Union, which is *sui generis*) will often have similar structures to the WTO law discussed here, and sometimes even incorporate by reference provisions of WTO law.

There are five main types of issues:

First, setting parameters for security characteristics of goods may violate national treatment, most favored nation (MFN) treatment, and even prohibitions on quotas under GATT and TBT. In relation to those parameters, importing states may recognize the regulation or certification provided by certain exporting states, also raising issues of MFN treatment.

Second, establishing characteristics of trusted manufacturers also raise the same legal issues, with the distinction that the regulatory focus is on the characteristics of the manufacturer, rather than those of the product itself.

Third, because IoT devices may be understood as hybrids between goods and services, similar issues of national treatment, MFN treatment, and market access under the GATS may be relevant.

Fourth, restrictions imposed in connection with government procurement, both in terms of the characteristics of the device and in terms of the characteristics of the manufacturer may raise issues under the GPA.

Finally, restrictions on investment in relation to IoT may violate market access requirements under bilateral investment treaties. These restrictions may either prohibit or set standards for all foreign investment, or focus on particular countries. If they focus on particular countries, or treat investment from certain countries differently, they may raise MFN issues.

Generally speaking, these measures only raise international legal issues when they are carried out by governments, or when they are carried out by private persons where the government has an international legal duty to prevent the private persons from taking the action at issue.[47]

International economic law was generally not written with cyber-operations in mind, and indeed, international economic law generally avoids involvement with security issues. This is the basis for the security exceptions discussed in this paper, and it is the basis for the political position taken by some states to the effect that they will not allow international economic law to restrain their national security-based actions.

However, security exceptions often have some textual limitations as to their availability, and so it is important to review international economic law in order to determine how cyber-operations may be restrained. Because negotiators did not have cyber-security in mind when they negotiated international economic law, these rules often do not apply clearly to cyber-security, and there is room for debate and litigation. In a sense, the question of the relationship between international economic law and cyber-security is a type of "fragmentation" issue, in which one

[47] *See* Shin Yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18 J. INT'L ECON. L. (2015).

area of international law inadvertently intersects another area of law or policy. It would be possible for states to enter into a cyber-security specific agreement, and to modify international economic law in order to provide that the international economic law defers to the cyber-operations agreement.

In the following subsections, I discuss WTO law rules that discipline national barriers to trade in goods or services, or that discipline government procurement for countries party to the GPA, as well as bilateral investment treaty rules relevant to restrictions on investment for IoT cybersecurity reasons. Subsequently, I discuss the security exceptions and general exceptions contained in each of these agreements, which might apply to relax these disciplines.

a. Trade in Goods: GATT and TBT Agreements

IoT products are, of course, goods. It is not certain whether software would be treated as a good or as a service in WTO law.[48] Different states take different positions on this issue, and the treatment depends in part on whether the software is incorporated into a physical medium or piece of equipment.

Nothing in GATT or the TBT would necessarily prevent an importing state from setting regulatory product standards consistent with cybersecurity with respect to imported IoT goods. However, under the GATT, states commit to provide national treatment and most-favored nation (MFN) non-discriminatory treatment to foreign goods in connection with domestic regulation. Therefore, less favorable treatment of imported goods from states deemed to pose more of a cybersecurity threat raises issues of MFN treatment. Under the TBT Agreement, states commit in addition not to impose technical regulations that are more trade restrictive than necessary to achieve a legitimate goal. They also commit not to impose technical regulations other than those incorporated in international standards, as defined, without an adequate justification.

Let us begin with the foundational GATT. Assume that a state imposes cybersecurity-based technical regulations on high risk IoT utilized to control factory processes. So long as these technical regulations do not discriminate between like products from foreign countries and domestically-produced products under Article III:4 of GATT, or between like products from different foreign countries under the MFN obligation of Article I of GATT, they are acceptable under GATT.

Discrimination under Article III:4 national treatment is understood as applying less favorable treatment to imported goods that are like products compared to more favorably treated domestic products. The WTO Appellate Body understands both the likeness of products and the possibility of less favorable treatment in terms of competition: are the imported and domestic products sufficiently in competition, and does the domestic regulation impair the competitive position of the imported products.[49] Note that the regulatory basis for distinguishing is not necessarily a part of the WTO approach to like products. Furthermore, even-handed regulation that has distinct

---

[48] For an analysis, *see* Althaf Marsoof, *A Case for* Sui Generis *Treatment of Software Under the WTO Regime*, 20 INT'L J. L. & INFO. TECH. 291 (2012).

[49] For a review of the relevant jurisprudence, *see* Joel P. Trachtman, *WTO Trade and Environment Jurisprudence: Avoiding Environmental Catastrophe*, 58 HARV. INT'L L. J. 273 (2017).

competitive effects may constitute less favorable treatment despite its even-handed character. Discrimination under Article I MFN is defined similarly (although its wording is somewhat different), comparing the treatment of imported products from one state to the treatment of like products from the complaining member state.

Note the implications of this analysis: blocking imports from a particular foreign state on the basis of that state's status as an adversary, or even that state's cybersecurity regulation regime, even if it is reasonable, could violate the GATT national treatment and MFN obligations.

Even if a violation of Article I or III is found, and as suggested above, it is entirely possible that even-handed regulation would be found to treat like products less favorably, a measure may be exempted if it satisfies the requirement for the exceptions contained in Article XX and Article XXI of GATT. Interestingly, there is no specific exception under either clause for measures motivated by privacy or consumer protection per se, but there are exceptions under Article XX for measures (i) necessary to protect human life or health, or (ii) necessary to secure compliance with laws relating, *inter alia*, to deceptive practices. The conditions for application of these exceptions are discussed in detail below.

It may be that in order to ensure cybersecurity of IoT products, states would have to regulate not only the product itself, but the process by which the product is produced.[50] Furthermore, states would need to regulate the way in which the device is connected to the internet, and surveil the safety of any updates or other instructions to the device. Because of the technical difficulty of control, it may even be that states would determine that only goods that are produced in states with similar political systems or with sufficient regulatory structures can be trustworthy, although the nationality or location of production is not a perfectly reliable proxy for trustworthiness.

It is not clear under the WTO rules of national treatment and MFN that states would be permitted to condition access to their markets on compliance with a specification of the way in which goods are produced, the way in which the production of goods is regulated in the state of production, or the politics of the state of production. The so-called "product-process distinction" or "product and production method distinction" (PPM) is still a contentious issue in WTO jurisprudence.[51]

On the other hand, if the goal of a requirement for production process supervision is to assure the safety of the product, as with supervision of slaughterhouses to ensure the safety of meat, it is arguable that the regulation is product regulation, carried out through supervision of the production process. In any event, even if these types of conditions may be found to violate the national treatment or MFN requirements, they might be permitted under the exceptions of Articles XX or XXI of GATT, described below.

---

[50] *See* Theodore Moran, *Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers*, Peterson Institute Policy Brief 13-11, dated May 2013, available at http://www.iie.com/publications/interstitial.cfm?ResearchID=2390.

[51] *See* Trachtman, *supra* note 49.

Interestingly, the TBT Agreement, which applies cumulatively with the GATT, also includes obligations of national treatment and MFN treatment, but lacks exceptions along the lines of Articles XX or XXI.[52] Thus it is possible that a measure would qualify for an exception under GATT, but still violate the TBT Agreement. The scope of the TBT national treatment requirement has been interpreted somewhat narrowly compared to that of GATT, excluding from violation measures that "stem exclusively from a legitimate regulatory distinction," in order to avoid invalidating a broader scope of national technical regulations than the GATT.[53] Article 2.1 of the TBT Agreement has been applied, for example, to find a violation in U.S. labeling requirements for dolphin-safe tuna, despite those requirements being otherwise even-handed in their application.[54] In that case, the Appellate Body found that the U.S. tuna labeling regime was insufficiently "calibrated" to different conditions in different areas, and thus could not be found to stem exclusively from a legitimate regulatory distinction."[55] Thus, national technical regulations applicable to IoT products will need to be designed with sufficient "calibration" to meet these requirements.

In addition, under Article 2(2) of the TBT Agreement, national technical regulations are not permitted to be "more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks non-fulfilment would create." National security requirements are explicitly included as "legitimate objectives." This necessity or proportionality test might be violated where there is a less trade restrictive alternative means available to achieve the legitimate objective. Again, this will impose important constraints on national technical regulations.

Furthermore, Article 2(4) of the TBT Agreement provides as follows:

> 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 fulfilment of the legitimate objectives pursued, for instance because of fundamental climatic or geographical factors or fundamental technological problems.

Thus, international standards, such as the network security provisions of ISO/IEC 27001,[56] to the extent that they constitute a "relevant international standard" in relation to a proposed or existing national measure, are required to be used as a basis for the national measure, except as specified in Article 2(4). This imposes some limitation on the flexibility available to states to impose

---

[52] Article 10.8.3 of the TBT Agreement contains a very narrow security exception dealing only with the disclosure of information. See the discussion below.

[53] *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, WT/DS406/AB/R, adopted 24 April 2012, at paras. 96-102.

[54] See Appellate Body Report, United States—*Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products, Recourse to Article 21.5 of the DSU by Mexico*, WTO Doc. WT/DS381/AB/RW, adopted 3 December 2015.

[55] *Id.*, ¶ 284.

[56] ISO/IEC 27033 Information technology — Security techniques — Network security (parts 1-3 published, parts 4-6 DRAFT), available at http://www.iso27001security.com/html/27033.html.

restrictions on importation of goods for cybersecurity purposes. However, the limitation would not seem to restrict the ability of a state to set a higher standard in order to achieve its nationally-determined "appropriate level of protection."

From a TBT Agreement standpoint, the only non-binding standard described in Part 2 that may qualify as an international standard in the sense of Annex 1.2 to that Agreement, by virtue of being promulgated by an international standardization body, would be the IOS reference architecture.[57] However, this seems specifically structured to avoid designation as a "standard." Nevertheless, at some point a more specific set of product characteristics may be elaborated by an international standard-setting body within the sense of Annex 1.2. The consequences of there being at this point in time no international standard are that (i) states have no obligation under Article 2(4) to use an international standard as a basis for their technical regulations, and (ii) states cannot take advantage of the rebuttable presumption of compliance with the TBT Agreement that arises under Article 2(5) if the state's technical regulation is in accordance with relevant international standards.

b. Trade in Services: The GATS Agreement

IoT goods might be understood as more than goods, but also as embedding a related service. Under WTO legal doctrine, WTO law relating to trade in services would be expected to apply cumulatively with the law relating to trade in goods, to the extent that there is an embedded or related services issue.[58] Thus, the GATS could apply to IoT goods.

GATS is in part a "positive list" agreement, meaning that some of its most significant disciplines only apply to the extent that a state has listed on its schedule of commitments the relevant service sector, in the relevant mode of international trade in services, such as "cross-border provision" (Mode 1) or "commercial presence" (Mode 3), and has not specified an applicable exception in its schedule of commitments. Recent commentary has begun to suggest that the services that are transmitted through their incorporation in goods represent a fifth mode of trade in services: Mode 5.[59] Mode 5 is not yet a legal category, so the services component of trade in IoT goods is likely to be understood as fitting within Mode 1: cross-border provision. It is also plausible that the services component of foreign investment in IoT goods manufacturing would be understood as Mode 3: commercial presence.

The disciplines that are dependent on scheduling are "national treatment," which is similar to the rule of national treatment non-discrimination in the GATT, and "market access," which is specifically defined to prohibit several specific types of quantitative restrictions, or other similar restrictions, on trade in services. For purposes of analysis, I assume that a state has

---

[57] *See* Appellate Body Report, *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, WT/DS381/AB/R, adopted 13 June 2012, para. 352.

[58] Appellate Body Report, *European Communities – Regime for the Importation, Sale and Distribution of Bananas*, WT/DS27/AB/R, adopted 25 September 1997.

[59] *See* Lucian Cernat, Trade rules and technological change: the case for mode 5 services, International Centre for Trade and Sustainable Development, November 4, 2015, available at https://www.ictsd.org/opinion/trade-rules-and-technological-change-the-case-for-mode-5-services.

commitments in these areas. All obligations discussed below are subject to security exceptions under Article XIV *bis* of GATS, addressed below.

The national treatment obligation under Article XVII of GATS requires each member to "accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers" (footnote omitted). Therefore, regulation would be required to be applied in an even-handed way to the foreign-origin services and service suppliers related to IoT goods, in comparison to domestic services and service suppliers. If foreign services or service suppliers, as a class, presented greater risks, it is not necessarily a violation of national treatment to treat them differently in a way that is responsive to the enhanced risk.

In *Argentina—Financial Services*,[60] the Appellate Body rejected claims by Panama against Argentina in connection with Argentina's measures designed to promote tax transparency. This case raised the important issue of whether members can condition access to their financial markets on particular aspects of the entering firm's home country regulation. Argentina argued that its measures restricted market access with respect to foreign firms that were based in "countries not cooperating for tax transparency purposes." The Appellate Body declined to rule on "whether the services and service suppliers of cooperative countries are 'like' the services and service suppliers of non-cooperative countries, or 'like' Argentine services and service suppliers." It thus declined to make a finding of violation of national treatment or MFN obligations. The possible relevance of this question, which is somewhat analogous to the PPM issue addressed above, to import policies that might be conditioned on the exporting country's IoT regulation, or geopolitical leanings, is important. Thus, if import restrictions were imposed on IoT goods originating in "countries not cooperating for cybersecurity purposes," there would be a serious question of their WTO legality.

The market access obligation under Article XVI of GATS, while expressly limiting the ability of states to impose quantitative restrictions, and certain other narrowly specified types of restrictions, has been interpreted by the WTO Appellate Body to apply to restrictions that might ordinarily be understood as *qualitative*. In the U.S.-Gambling case, the Appellate Body found that restrictions on cross-border internet gambling services violated this restriction.[61] So it is possible that cybersecurity restrictions applied to services embedded in IoT goods might similarly be found to violate this restriction.

Article II of GATS contains an MFN obligation, which applies regardless of scheduling. This MFN obligation may make it illegal to treat service providers of allies or other trusted countries differently from service providers or services from other states. The analysis would be similar to that in connection with goods under GATT.

---

[60] Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, WT/DS453/AB/R and Add.1, adopted 9 May 2016.

[61] Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, adopted 20 April 2005.

Finally, Article VI of GATS provides a complex discipline on domestic regulation of imported services. In essence, WTO members are not permitted to apply technical standards that nullify or impair specific commitments in a manner that is more burdensome than necessary to ensure the quality of the service and could not reasonably have been expected at the time the specific commitments were made. Interestingly, the latter criterion might be satisfied by virtue of technological change.

c. Government Procurement

Importantly, as noted above, the GPA is a plurilateral agreement. Plurilateral trade agreements do not create either obligations or rights for the WTO members that have not accepted them. The GPA applies to procurement for governmental purposes of both goods and services, and it is a positive list agreement, meaning that its obligations are dependent on scheduling of the covered products, services, and government entities.

The GPA also includes in Article IV obligations of national treatment and MFN treatment. On this basis, a member of the GPA cannot exclude suppliers that are nationals of other GPA members from tendering, or treat them or their products or services less favorably than they treat local suppliers or suppliers from third GPA members. Therefore, it may be illegal to exclude suppliers on the basis of nationality.

In addition, a procuring entity is required under Article VIII to limit conditions for participation to those that are essential to ensure that the supplier has the legal and financial capacities and the commercial and technical abilities to undertake the relevant procurement. This obligation may make it difficult to impose cybersecurity conditions for participation.

States subject to these obligations would want to be sure to include cybersecurity parameters as part of the technical requirements relating to their procurement. Finally, Article X of the GPA states that "a procuring entity shall not prepare, adopt or apply any technical specification or prescribe a conformity assessment procedure with the purpose or the effect of creating unnecessary obstacles to international trade." Under this requirement, technical specifications and conformity assessment intended to achieve cybersecurity goals must be the least restrictive alternative to achieve the goal.

d. Security Exceptions

Article XXI of GATT, Article XIV *bis* of GATS, and Article III of the GPA provide security exceptions. Interestingly, these exceptions have different scopes of application. To the extent that these exceptions may apply, they would excuse measures that violate the provisions discussed above. Of course, the exceptions only become relevant if there is a violation.

> GATT. Article XXI (b) provides in relevant part that nothing in the GATT "shall be construed [...] to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests (i) [...]; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military

> establishment; or (iii) taken in time of war or other emergency in international relations [...]"
> GATS. Article XIV *bis* of GATS provides in relevant part that nothing in the GATS "shall be construed [...] to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests: . . . (ii) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment; or (iii) taken in time of war or other emergency in international relations [...]."
> GPA. Article III of the GPA provides that "[n]othing in this Agreement shall be construed to prevent any party from taking any action [...] that it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes."

Curiously, while the TBT Agreement contains a provision providing that Members shall not be required to furnish any information, the disclosure of which they consider contrary to their national security interests, it does not provide a security exception similar to those contained in the other agreements referenced above. While there may be some argument that the GATT security exception applies by implication to TBT measures, this argument is unlikely to be successful.

I will review the potential applicability of these exceptions in turn.

Some states have argued that the GATT Article XXI(b) security exception as "self-judging,"[62] meaning (i) that each state decides for itself whether to use the exception, and (ii) that the rationale for its use is not subject to dispute settlement. However, this perspective has, at the date of this writing, been rejected by a WTO dispute settlement panel, and the language of Article XXI(b) suggests a more nuanced approach.[63] The more nuanced approach adopted by the panel in Russia—Traffic in Transit recognizes that the existence of the enumerated conditions is not self-judging; rather, what is self-judging is whether the national measure is *necessary* for the protection of the state's essential security interests in response to the existence

---

[62] *See, e.g.,* George Dian-Balán, *On Fissionable Cows and the Limits to the WTO Security Exceptions*, 14 GLOBAL TRADE & CUSTOMS J. 2, 10 (2018); Roger P. Alford, *The Self-Judging WTO Security Exception*, 3 UTAH L. REV. 697 (2011); Stephan Schill & Robyn Briese, *'If the State Considers': Self-Judging Clauses in International Dispute Settlement*, 13 MAX PLANCK Y.B. OF U.N. L. 61 (2009); William W. Burke-White & Andreas von Staden, *Investment Protection in Extraordinary Times: The Interpretation and Application of Non-Precluded Measures Provisions in Bilateral Investment Treaties*, 48 VA. J. INT'L L. 307 (2008); Dapo Akande & Sope Williams, *International Adjudication on National Security Issues: What Role for the WTO?*, 43 VA. J. INT'L L. 365 (2003); Wesley A. Cann, Jr., *Creating Standards and Accountability for the Use of the WTO Security Exception*, 26 YALE J. INT'L L. 213 (2001); Hannes L. Schloemann & Stefan Ohlhoff, *'Constitutionalization' and Dispute Settlement in the WTO: National Security as an Issue of Competence*, 93 AM. J. INT'L L. 424 (1999).

[63] Panel Report, Russia—Measures Concerning Traffic in Transit, WT/DS512/R, April 5, 2019, available at https://www.wto.org/english/tratop_e/dispu_e/512r_e.pdf (Russia—Traffic in Transit Panel Report).

of the relevant enumerated condition.[64] The panel's reading was that the necessity is subjective, but the existence of the war or other emergency is objective.[65]

Furthermore, even the "it considers" modifier does not necessarily mean there can be no judicial review. Rather, the panel in Russia—Traffic in Transit determined that, even though necessity is subjective, judicial review may address whether the state in good faith considers its measure necessary as prescribed.[66] The state's determination is subject to a duty of good faith in international law, pursuant, inter alia, to Articles 26 and 31, as well as the third recital, of the Vienna Convention on the Law of Treaties.

In addition, "essential security interests," while within the subjective determination of the invoking state,[67] "relate to quintessential functions of the state"—"protection of territory and its population from external threats, and the maintenance of law and public order internally."[68] Under this approach, high risk IoT would seem to be covered, but low risk IoT would not. The panel stated that, while the determination of essential security interests is within the judgment of the invoking state, the invocation must be made with sufficient specificity in the context to demonstrate its veracity.[69]

The panel in Russia—Traffic in Transit examined the important question whether a "war or other emergency in international relations" exists. The panel interpreted this language as follows:

> An emergency in international relations would, therefore, appear to refer generally to a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state. Such situations give rise to particular types of interests for the Member in question, i.e. defence or military interests, or maintenance of law and public order interests.[70] (footnotes omitted)

It also found that "political or economic differences between Members are not sufficient, of themselves."[71] The circumstances under which ordinary precautions against cyber-attack may fall within this definition is uncertain. However, it is possible that the need to defend against a rising risk of catastrophic cyberattack through high risk IoT might well be understood as a type of crisis, amounting to an "emergency in international relations."

---

[64] *Id*., para. 7.101. *See* also Dapo Akande & Sope Williams, *International Adjudication on National Security Issues: What Role for the WTO?*, 43 VA. J. INT'L L. 365, 399-400 (2003).
[65] *Id. See* European Union Third Party Written Submission, ¶¶ 41–45, *Russia – Measures Concerning Traffic in Transit* (DS512); Schloemann & Ohlhoff, *supra* note 62, at 446; Michael J. Hahn, *Vital Interests and the Law of GATT: An Analysis of GATT's Security Exception*, 12 MICH. J. INT'L L. 558, 584 (1991).
[66] Russia—Traffic in Transit, *supra* note 63, paras. 7.132-7.138.
[67] *Id.*, para. 7.131.
[68] *Id.*, para. 7.130.
[69] *Id.*, para. 7.134-135.
[70] *Id.*, para. 7767.76.
[71] *Id.,* para. 7757.75.

There is another potentially relevant sub-paragraph of Article XXI(b): subparagraph (ii), "relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment." Here we have no adjudicative interpretation, but it is plausible that high risk IoT might be understood in context as at least a potential implement of war, and thus covered by this provision. Furthermore, *export controls* imposed by the U.S. and other countries with respect to not just arms, but dual use goods, seems consistent with an understanding of Article XXI(b)(ii) that includes *import controls* on at least high risk IoT. For both import controls and export controls, the decision of the panel in Russia—Trade in Transit would require that the restrictions be imposed in good faith.

Note that the national security exception would appear to be arguably available, either under Article XXI(b)(iii) (emergency) or Article XXI(b)(ii) (implements of war), or both, with respect to high risk IoT, provided that the restrictions are applied in good faith. It is more difficult to see the application of the national security exception to low risk IoT. I discuss below the potential application of the general exceptions in Article XX of GATT to low risk IoT.

At the time that this paper was prepared, the scope of the national security exception was being challenged in additional cases beyond the Russia—Trade in Transit case.[72] These cases involve measures taken by the U.S. and the United Arab Emirates. The decisions in these cases, and Appellate Body determinations, if any, will further clarify questions of the justiciability, and scope, of the GATT national security exception.

Article XIV *bis* of GATS contains identical relevant language, and can be expected to raise the same interpretive issues in our context as Article XXI of GATT.

On the other hand, the security exception contained in Article III of the GPA is remarkably limited. First, we have a similar interpretive question to that addressed with respect to Article XXI—to what part of Article III of the GPA does "that it considers necessary" refer? However, the scope of action is triggered by the "procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes."

While this provision would allow an exception for governmental purchases of war materials or other procurement indispensable for national security or defense purposes, it is questionable whether this phrasing can be extended to cover procurement of non-military or intelligence IoT goods that are not themselves war materials or indispensable for security. It is possible that procurement of high risk IoT itself could be understood as "indispensable for national defence" in some circumstances, but that would often be an extension from what one would ordinarily think of as indispensable for national defense. It is not the procurement itself that is likely to be understood as indispensable, but the secure characteristics of the goods or embedded services

---

[72] *United Arab Emirates – Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Rights*, *in* Minutes of Meeting Held in the Centre William Rappard on 22 November 2017, ¶¶ 3.1-3.15, WTO Doc. WT/DSB/M/404 (Mar. 6, 2018). There are several cases against the U.S. steel and aluminum tariffs, including DS548: United States — Certain Measures on Steel and Aluminium Products, panel composed on January 25, 2019.

procured. So, first, it is unlikely, in light of Russia—Traffic in Transit, that Article III of the GPA is completely self-judging, and second, the trigger events seem more limited than those contained in Article XXI of GATT.

Indeed, while the public procurement covered by the GPA presents a major issue in terms of cybersecurity threats to or through public services or other public infrastructure, it seems to provide the narrowest exception. Interestingly, while the GPA applies cumulatively with the GATT (and GATS), there does not appear to be a basis for arguing that the security exception of the GATT is available for violations of GPA obligations.

To sum up on the role of the security exception in the WTO system, we must first say that the long-standing uncertainty regarding the justiciability and scope of self-judging character of the security exceptions has been partially, and perhaps tentatively, addressed by the panel decision in Russia—Trade in Transit. With respect to GATS, we would have to examine individual countries' schedules of commitments in order to determine whether they have taken additional security exceptions within these schedules. The TBT Agreement does not contain a relevant security exception, and so in order to have a security exception with respect to obligations contained in the TBT Agreement, it would be necessary to argue that the GATT security exception somehow applies within this other agreement, despite the fact that Article XXI of GATT says that "nothing in *this* agreement shall be construed to prevent [...]"[73] With respect to government procurement, we have a security exception of narrower scope, which, for example, would not appear clearly to cover cybersecurity-based restrictions in public procurement of network equipment or railway controls if they were designed in a way that violated another provision of the GPS Agreement.

e. General Exceptions

In a pattern similar to that observed with respect to the security exception, each of the GATT, GATS, and GPA Agreements contains a general exception that may be applicable to cybersecurity defense operations. The TBT Agreement contains no explicit general exception. GATT Article XX has been the basis for significant litigation in the WTO, and there has been some litigation also over the exceptional provision of GATS, Article XIV. The language of these exceptions is quite similar, and can be expected to be interpreted similarly. In this subsection, I will focus on GATT Article XX.

---

[73] No WTO tribunal has examined whether the Article XXI exception would be available to defend against claims under the TBT Agreement. However, in the similar context of the Article XX general exceptions, discussed below, the Appellate Body has declined to apply Article XX as an exception with respect to obligations under the TBT Agreement. Appellate Body Report, *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, WT/DS406/AB/R, adopted 24 April 2012, at paras. 96-102. However, it has interpreted the TBT Agreement obligations narrowly in order to reflect the values of the Article XX exception. In light of the Appellate Body's decision in *China—Raw Materials*, members may only expect to rely directly on GATT Article XX exceptions when the provisions of another covered agreement explicitly refer to the GATT. See Appellate Body Report, *China—Measures Related to the Exportation of Various Raw Materials*, WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, adopted 30 January 2012, at paras. 303-306.

GATT Article XX provides in relevant part as follows:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any contracting party of measures:
> [...]
> (b) necessary to protect human, animal or plant life or health [...]
> (d) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement, including those relating to . . . the prevention of deceptive practices.

Focus first on enumerated clause (b). Could restrictions on imports of IoT goods (or related services under the similar language of GATS Article XIV) be necessary to protect human life or health? This provision is definitely not self-judging, but it is easy to see many IoT cybersecurity defensive measures, especially those that relate to high risk IoT, as "necessary to protect human life." Many low risk IoT measures would not fall within this exception.

However, enumerated clause (d) may include a number of rules relating to low risk IoT. Where low risk IoT is a potential tool of violation of other GATT-consistent laws, such as consumer protection laws, enumerated clause (d) would appear to be available, subject to the "necessary" qualification, and to the "chapeau," requiring that the measure not be used as a means of arbitrary or unjustifiable discrimination. Here, we can imagine a dispute about whether distinctions between Chinese-sourced IoT goods and British-sourced goods is arbitrary or unjustifiable.

The word "necessary" in this context has been interpreted extensively. In some cases, the Appellate Body has explicitly interpreted this provision as requiring a balancing approach. In others, it has appeared to back off of a full balancing approach by permitting the member to choose its "level of protection" and then validating the national measure if this level cannot be reached through a less trade-restrictive, reasonably available, alternative means.

The Appellate Body most notably formulated and applied a judicial balancing approach in a case involving a requirement of the Republic of Korea that retailers make a choice of only selling Korean or foreign beef.[74] In *U.S.-Gambling*, a GATS Article XIV case, the Appellate Body confirmed that a "'reasonably available' alternative measure must be a measure that would preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued."[75]

While GATS Article XIV largely tracks GATT Article XX, it adds an enumerated clause that includes measures "necessary to protect . . . public order," invokable "only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society." (The elided

---

[74] *See* WTO Appellate Body, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef* WT/DS161/AB/R & WT/DS169/AB/R, adopted 11 December 2000. *See also Dominican Republic – Measures Affecting the Importation and Internal Sale of Cigarettes* WT/DS302/AB/R, adopted 25 April 2005, at para. 70 (affirming the "weighing and balancing" of these factors).

[75] Appellate Body Report, *U.S.—Gambling*, *supra* note 61, at para. 308.

words are "public morals," which are included in a similar provision of GATT.). This enumerated clause may allow exceptions beyond those available under GATT.

The general exception contained in Article III:2 of the GPA essentially tracks the provisions of Article XX of GATT. Therefore, for procurement covered by the GPA, states may derogate from their GPA obligations in order to effect measures necessary to protect human life or health, etc. In addition, the GPA seems to permit procuring states to establish specifications for goods or services, conditions for participation, or bidder qualification requirements, that may relate to cybersecurity concerns. As mentioned above, with respect to specifications, Article X:1 provides that "a procuring entity shall not prepare, adopt or apply any technical specification or prescribe any conformity assessment procedure with the purpose or the effect of creating unnecessary obstacles to international trade." So, a necessity test, likely to be similar to that applied under Article XX of GATT, would apply to cybersecurity-based technical specifications.

For each of these exceptions to be available, it is necessary that the additional conditions specified in the relevant "chapeau" also be satisfied. For example, the chapeau of Article XX of GATT requires that the relevant measure not "constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail." This would raise again the question of whether it is permissible to treat goods or services exported by an adversary or a state that did not cooperate in cybersecurity differently. In order to avoid charges of arbitrariness or unjustifiability, regulation would need to be designed proportionately, and would benefit from prior negotiation with the exporting state.[76]

f. Investment Law

States have often in the past imposed restrictions on foreign investment for national security reasons. With respect to IoT goods, security threats can just as readily be posed by domestically-produced goods produced by foreign owned (or domestically-owned) factories. The U.S. has recently tightened its controls on foreign investment.[77]

International investment law is drawn partially from customary international law, but it is increasingly dominated by bilateral investment treaties (BITs), including the portions of free trade area agreements that are designed to emulate a BIT. BITs generally protect foreign investment originating in the partner country, and sometimes also include market access guarantees providing permission for entry of foreign investment from the partner country. The market access guarantees often are framed as requirements of national treatment with respect to the establishment of the investment. BITs that include these market access guarantees may raise issues regarding whether a host state may exclude certain foreign investors from certain industries in order to carry out a cyber-security program, or establish cyber-security-based conditions for market entry.

---

[76] Appellate Body Report, United States—Import Prohibition of Certain Shrimp and Shrimp Products, WTO Doc. WT/DS58/AB/R, ¶¶ 166, 171 (adopted Nov. 6, 1998).

[77] Foreign Investment Risk Review Modernization Act of 2018, tit. XVII, Pub. L. No. 115-232, Aug 13, 2018, 132 Stat. 1638. *See* Frédéric Wehrlé & Joachim Pohl, *Investment Policies Related to National Security*, at 10, OECD Working Papers on Int'l Investment 2016/02 (2016).

In addition, changes in technology or perception result in changes in cyber-security concerns that may lead to ejection of, or the imposition of more stringent conditions on, foreign investors. These measures may raise issues under BITs provisions that protect foreign investment from discrimination or mistreatment *after* establishment.

While each BIT is different, some states, such as the U.S., have model BITs with which they begin negotiations. For purposes of illustration, I will discuss the relevant provisions of the 2012 U.S. model BIT.[78] The national treatment provision of Article 3 of the 2012 U.S. model BIT (National Treatment) provides as follows:

1. Each Party shall accord to investors of the other Party treatment no less favorable than that it accords, in like circumstances, to its own investors with respect to the establishment, acquisition, expansion, management, conduct, operation, and sale or other disposition of investments in its territory.
2. Each Party shall accord to covered investments treatment no less favorable than that it accords, in like circumstances, to investments in its territory of its own investors with respect to the establishment, acquisition, expansion, management, conduct, operation, and sale or other disposition of investments.

Note that Article 3(1) provides for national treatment as to establishment—this is a commitment to market access for investment. Article 3 also provides for national treatment for foreign investors and their investments—treatment no less favorable than that accorded domestic nationals. So, the question raised in connection with restrictions on investment in IoT manufacturing is whether exclusions or special conditions applied to foreign investors or their investments would constitute less favorable treatment. Current jurisprudence is somewhat uncertain as to the extent to which differential treatment can be justified in a way that avoids its characterization as "less favorable."[79] However, where the basis for the different treatment is based merely on different nationality, as opposed to different risk characteristics, it would be unlikely to withstand national treatment scrutiny. Similar issues would arise under the "most favored nation" treatment obligation of Article 4, where a state determines to treat foreign investors or investments from different countries differently in connection with cybersecurity risk.

In addition, Article 5 of the 2012 U.S. model BIT provides that "each Party shall accord to covered investments treatment in accordance with customary international law, including fair and equitable treatment and full protection and security." The scope of fair and equitable treatment and full protection and security may include restrictions on foreign investments in IoT activities, for example where a foreign investor or investment is subjected to costly requirements or restraints based on cybersecurity concerns. While the 2012 U.S. model provides quite restrictive definitions of fair and equitable treatment and full protection and security—referring to due process and police protection—other investment treaties do not restrict the scope of these obligations in this way.

---

[78] 2012 U.S. Model BIT, available at http://www.state.gov/e/eb/ifd/bit/index.htm.

[79] *See* Nicolas DiMascio & Joost Pauwelyn, *Nondiscrimination in Trade and Investment Treaties: Worlds Apart or Two Sides of the Same Coin,* 102 AM. J. INT'L L. 48 (2008).

Many BITs include clauses making the protection of essential security interests a defense, justifying an action of the state that would otherwise be prohibited. For example, Article 18 (Essential Security) of the 2012 U.S. model BIT contains the following security exception:

> Nothing in this Treaty shall be construed:
>
> 1. to require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or
> 2. to preclude a Party from applying measures that it considers necessary for the fulfillment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.

Note that this model has a "self-judging" or subjective feature similar to that found in the WTO provisions. However, most BITs that contain security exceptions do not contain language such as "that it considers necessary,"[80] with the result that whether a measure is necessary for the protection of the acting state's essential security interests is an objective question, and is not self-judging.

Indeed some BITs do not contain security exceptions at all.[81] Given the concerns described above that defenses against cyberattack through IoT goods may violate other provisions of investment liberalization treaties, states may wish to review their policy with respect to the need for security exceptions. Note that where a treaty includes no security exception, a customary international law defense of necessity, based on security needs, may still be available.[82] However, the customary international law necessity defense requires that the non-compliance "(a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole."[83]

On the other hand, the OECD *Codes of Liberalisation of Capital Movements and of Current Invisibles Operations,* a legally binding agreement among OECD members but now open to other states, in Article 3, provides that its provisions "shall not prevent a Member from taking action which it considers necessary for the" . . . "ii) protection of its essential security interests […]"

A BIT security exception was considered in connection with arbitration cases relating to Argentina's 1999-2002 economic crisis. Article XI of the Argentina-U.S. BIT provides:

---

[80] Katia Yannaca-Small, *Essential Security Interests under International Investment Law*, chapter 5 in INTERNATIONAL INVESTMENT PERSPECTIVES: FREEDOM OF INVESTMENT IN A CHANGING WORLD 93-134, 94 (OECD 2007).

[81] *Id.* at 98.

[82] *See* the discussion in *id.*, at 98-100.

[83] International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 25 (2001), available at http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf .

> This Treaty shall not preclude the application by either Party of measures necessary for the maintenance of public order, the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security or the protection of its own essential security interests.[84]

Note that this provision contains no indicator that it is "self-judging," and indeed the tribunals that considered it indicated that without explicit language making the security exception self-judging, it is not.[85]

In a number of the Argentina cases, the issue came up whether economic crisis could be a basis for invocation of this type of security exception. This question is important to the cybersecurity issue, because cybersecurity may also relate to a type of security beyond kinetic warfare, including geoeconomic conceptions of factors contributing to security. Several of the tribunals rejected the argument that Article XI was only applicable in circumstances amounting to military action and war.[86] One stated that, to find that a severe economic crisis could not constitute a national security issue was "to diminish the havoc that the economy can wreak on the lives of an entire population and the ability of the Government to lead."[87] For the same reasons, this type of provision might be interpreted to be invokable in order to avoid cyber-attack based havoc. The Argentina tribunals varied with respect to their interpretation of the degree of severity of disruption that would be necessary in order to invoke the security exception.[88]

g. Conclusion

The following table summarizes the issues and likely disposition with respect to trade in goods:

---

[84] Treaty between the United States of America and the Argentine Republic concerning the reciprocal encouragement and protection of investment, signed 14 November 1991, entered into force 20 October 1994, available at: http://www.unctadxi.org/templates/DocSearch____779.aspx.

[85] *E.g.,* CMS Gas Transmission Company v. Argentine Republic, ICSID Case No. ARB/01/8, Award, 12 May, 2005; 29. LG&E Energy Corp., L&E Capital Corp., LG&E International Inc v. Argentine Republic, ICSID Case No. ARB/02/1, Decision on Liability, 3 October 2006; 30. Enron Corporation Ponderosa Assets, L.P. v. Argentine Republic, ICSID Case No ARB/01/3, Award, May 22, 2007. *See also* Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v US), Merits, 1986 ICJ 14, 116; Oil Platforms (Iran [Islamic Rep. of] v United States) 1996 ICJ 803, 20.

[86] *See, e.g., Continental Casualty Co. v. Argentine Republic*, ICSID Case No. ARB/03/9, Award, ¶¶ 181 (Sept. 5, 2008); *LG&E Energy Corp. v. Argentine Republic*, ICSID Case No. ARB/02/1, Decision on Liability, ¶¶ 332 (Oct. 3, 2006); *Sempra v. Argentina*, ICSID Case No. ARB/02/16, Award, ¶ 374 (Sept. 18, 2007); *CMS Gas Transmission Co. v. Argentine Republic*, ICSID Case No. ARB/01/8, Award, ¶¶ 359 (Apr. 25, 2005); *Enron Corp. v. Argentine Republic*, ICSID Case No. ARB/01/3, Award, ¶¶ 324–26 (May 22, 2007); *El Paso Energy Corp. v. Argentine Republic*, ICSID Case No. ARB/03/15, Award, ¶¶ 563–73 (Oct. 31, 2011).

[87] LG&E International Inc. v. Argentine Republic, ICSID Case No. ARB/02/1, Decision on Liability, 3 October 2006, para. 238.

[88] *See* United Nations Conference on Trade and Development, The Protection of National Security in IIAs, UNCTAD/DIAE/IA/2008/5, 9-10 (2009).

	Possible GATT violations	GATT security exception	GATT general exception	Possible TBT violations	No TBT security or general exception
Low Risk IoT	Little need to violate national treatment or MFN	XXI probably unavailable	XX(d) probably available	2.1 (national treatment or MFN) 2.2 (proportionality) 2.4 (use international standards)	
High Risk IoT	III:4 I (MFN)	XXI probably available	XX(b) possibly available	2.1 2.2 2.4	

With respect to low risk IoT, WTO law permits states to establish technical regulations that will sufficiently address cybersecurity concerns, subject to significant constraints under the TBT Agreement. States will have no need to discriminate in real terms with respect to low risk IoT. However, note that the WTO Appellate Body has found that where products that are competitively "like" experience impaired market access, there can be a violation of the relevant anti-discrimination provisions. In the TBT context, there is no violation if the difference in treatment "stems exclusively from a legitimate regulatory distinction.

There will be important incentives to harmonize these technical regulations among states, in order to avoid the inefficient need for different software, and even hardware, in different markets, but these incentives may not be distributed evenly enough to induce agreements to harmonize. In addition, different types of IoT products will require different technical regulations in order to customize the requirements to the degree of risk and to the structure of the particular type of IoT device. With respect to foreign investment law, similarly, technical regulations should be sufficient to address low risk IoT cybersecurity concerns. Despite the relative tractability of low risk IoT concerns, it is possible that states would protect their markets through excessive application of national security exceptions.

The more difficult problems are posed by high risk IoT devices. Here, states may bar imports or bar imports from specified countries or companies deemed to present a security risk. They may develop rules that certify suppliers as trusted based in part on their location or ownership, or simply impose higher standards on IoT devices produced by certain suppliers based on location or ownership. These distinctions, though reasonable from a security perspective, may violate national treatment or MFN obligations, or proportionality requirements under the TBT Agreement. They may be justifiable as to GATT under the GATT general exceptions or under the GATT national security exception. To the extent that the national security exception in GATT is understood as self-judging and non-justiciable (contrary to the panel decision in Russia—Traffic in Trade), these distinctions may be applied without restraint.

The degree to which WTO law and international investment law may restrict the ability of states to establish cybersecurity defenses against risks of imported high risk IoT goods or related services, or against investment in domestic production facilities for high risk IoT goods, is dependent on the scope of relevant security exceptions, which, even after Russia—Traffic in Transit, is somewhat uncertain. The language of these exceptions was not well-designed for application to high risk IoT goods. If the exceptions are interpreted broadly, then state restrictions on imports or investment will not be required to be precise, or well-designed to address the tradeoff between trade and security. Thus, the level of restrictions may be overbroad. Furthermore, restrictions may be motivated by protectionism, and the existing law does not provide a reliable mechanism to discern protectionist from authentic security motivations. Finally, restrictions may be motivated by geoeconomic competition, and therefore may be overbroad from the standpoint of cybersecurity for this reason.

So, unless the jurisprudence develops to provide more specific constraints on use of the security exception, or states are able to agree on a legal and institutional arrangement beyond the existing trade and investment law systems to verify the security of high risk IoT goods, much trade will be impeded, and relevant investment will be discouraged. Therefore, it is useful to imagine what the structure of a legal and institutional arrangement to verify security of IoT goods might be, and how it might interact with the trade and investment law regimes.

It might appear that the bargaining power in negotiating such a regime lies with the importing states, but since imports are valuable to the importing state both on the consumption and on the supply chain-based production side, both sides can be expected to be interested in establishing an appropriate regime. Furthermore, many relevant states will be both an importer and an exporter of IoT goods, so that reciprocity will be an important incentive. Finally, states engaged in geoeconomic competition may be willing to utilize an appropriate regime to ameliorate the security competition, much the way arms control agreements have done so.

5. Developing Legal and Institutional Responses

There is no doubt that different types of risk, and different types of technical context, will require different types of cybersecurity and trade law responses. There will likely be no circumstances in which a producer from a security competitor country will be permitted to supply IoT weapons or other core security devices. National discretion in this area is clearly protected by the security exceptions in Article XXI(b)(ii) of GATT, Article XIV(b)(ii) of GATT, and Article III(1) of the GPA.

Beyond that, as we move from government procurement of core security devices and private procurement of central critical infrastructure the disruption of which could be devastating, toward lesser security threats, it may be possible to develop systems by which producers located in foreign states, or controlled by foreign states, are permitted market access. This section reviews some of the possible structures that might be included in such systems, and suggests how they might comply with international law.

The core technical problem of ensuring IoT security lies in evaluating the initial and updated software installed on the device (hardware is easier to evaluate). This can be achieved through trust or verification, although both will be subject to hacking.

- **Trust**. As to trust, the focus is on evaluating the person controlling the software. This is not a simple question of nationality of suppliers, but is complicated by the need to include (i) ownership, (ii) supply chains, and (iii) employees in the determination of trust. Importantly, less trust will be required for low risk IoT than for high risk IoT.
- **Verification**. Verification focuses on the software itself, rather than the controlling person. Like the British HCSEC approach, it involves setting up a sufficiently trusted evaluator with the technical capabilities needed to evaluate software to be installed initially or upon update, and also with the ability to ascertain whether the software actually installed in the subject devices matches the software that was evaluated.
- **Hacking**. IoT devices, by virtue of being connected to the internet, are vulnerable to hacking attacks. Therefore, one critical facet of verification will involve ascertaining that the level of vulnerability to hacking of software and hardware comprising the IoT device is at acceptable levels.

For low risk IoT, where by definition the cost of a security breach is not catastrophic, trust, based on certification of suppliers, combined with verification or other assurance of the security design and sufficiency of anti-hacking protections, may be sufficient protection. Indeed, for certified suppliers of low risk IoT, the verification might consist of imposition of security standards such as those described in part 3 above, with some spot-checking by regulators or perhaps merely a liability standard for damages arising from failure to meet those standards.[89] For certified suppliers of high risk IoT, partly because so much is at stake, spot-checking or liability standards may not provide sufficient assurance, so that a higher level of verification is required.

For non-certified suppliers, more complete verification of security design and anti-hacking protections will be required in the case of low risk IoT, but at a level below that which would be necessary for high risk IoT. This intermediate level of verification may involve assessment of the trustworthiness of the supplier and its home state. For high risk IoT, complete verification will be essential, but may be carried out at a reduced level of scrutiny for certified suppliers. The greatest verification will be reserved for non-certified suppliers of high risk IoT.

Thus, a risk-protection matrix might resemble the following:

	Certified Supplier	**Non-Certified Supplier**
Low Risk IoT	Light verification of security design and anti-hacking	Intermediate verification of security design and anti-hacking
High Risk IoT	Intermediate verification of security design and anti-hacking	Maximum verification of security design and anti-hacking

[89] *See* Ikenson, *supra* note 2.

a. Low Risk IoT: The SPS and Sarbanes Oxley Analogies

As indicated by the review in Part 3 of processes and standards for making consumer IoT secure, (i) the appropriate security measures will depend on the technical context and the degree of risk, and (ii) some degree of harmonization of requirements will be useful so that uniform products can be marketed around the world. To the extent that harmonization of requirements is established, it will be easier to agree also on equivalence and mutual recognition arrangements. Here, "equivalence" should be understood as acceptance of foreign regulatory standards as satisfactory for importing country regulatory purposes. "Mutual recognition" should be understood in its narrow sense as acceptance of foreign certification of satisfaction of regulatory standards as satisfactory for importing country purposes. Note that mutual recognition will depend on the establishment of sufficient trust, and thus will be easier with low risk IoT than with high risk IoT.

Furthermore, because by definition low risk IoT does not provide great incentives for mounting an effective attack, and because by definition states can sustain an attack without grievous consequences, perfect security is unnecessary, and would be likely to be excessively costly.

The risk profile associated with low risk IoT, the manner in which harms may be transmitted, the possibility of harmonization, and the possibility of equivalence, and mutual recognition, are somewhat analogous to the risk profile presented by disease causing agents or contaminants in food, and the multilateral response. The relationship between food safety risks and trade is addressed in a nuanced manner under the WTO Agreement on Sanitary and Phytosanitary Measures (the SPS Agreement). One analogy between the SPS Agreement context and the IoT software context is that verification of safety may involve establishing parameters of trust for producers, or actually surveilling the production, of both food and IoT software.[90]

In addition, in connection with carrying out audits of public companies to ensure against fraud in the securities markets, the Sarbanes-Oxley Act of 2002 (Sarbox) requires that the auditor of a company's financial statements, whether a U.S. national or not, must be registered with U.S. authorities (the Public Company Accounting Oversight Board, or PCAOB) and subject to their jurisdiction. Registered auditors are required to undergo periodic PCAOB inspections to examine compliance with U.S. law and professional standards, including requirements of independence. This also presents some characteristics analogical to security in connection with low risk IoT goods.

I discuss the SPS Agreement and the Sarbox analogies in turn.

i. SPS, Harmonization, Equivalence, Mutual Recognition, and Foreign Inspections

[90] *See* SPS Agreement, Annex C, para. 2: "Where a sanitary or phytosanitary measure specifies control at the level of production, the Member in whose territory the production takes place shall provide the necessary assistance to facilitate such control and the work of the controlling authorities."

Under the SPS Agreement, WTO members are permitted to impose safety requirements on imported food. These national safety requirements are subject to disciplines similar to those imposed under the TBT Agreement described above, including the obligation to base national safety standards on international standards, such as those developed by the Codex Alimentarius. Under Article 3 of the SPS Agreement, members must base their regulation on Codex Alimentarius standards unless "there is a scientific justification, or as a consequence of the level of sanitary or phytosanitary protection a member determines to be appropriate" in accordance with the SPS Agreement."

In addition (and this has some similarity also to provisions of the TBT Agreement), the SPS Agreement requires members to accept the sanitary or phytosanitary (SPS) measures of other members as equivalent, "if the exporting Member objectively demonstrates to the importing Member that its measures achieve the importing Member's appropriate level of sanitary or phytosanitary protection."[91]

As an example of action in this field, the U.S. Food and Drug Administration (FDA) (i) engages in harmonization efforts largely by working with other governments to set standards through the Codex Alimentarius Commission, (ii) engages in "systems recognition", whereby the FDA makes a determination to "recognize" that a foreign food safety regulatory system achieves food safety outcomes comparable to those of the U.S., and engages in "equivalence" efforts whereby the FDA recognizes that a foreign food safety regulatory system, while having different mechanisms, achieves the same level of health protection as does the U.S.[92] (The terms "recognition" and "equivalence" are used by the FDA in slightly different senses from those adopted in this paper.)

Note that under the SPS Agreement, members are required to accept equivalence if the exporting member provides objective evidence that its regime achieves the importing member's appropriate level of protection. This international law obligation leaves little room to distinguish by reference to overall trust, or other parameters. A cybersecurity regime for low risk IoT might be designed to permit some distinctions of that nature. The TBT Agreement, which would apply to IoT products, merely requires that "Members shall give positive consideration to accepting as equivalent technical regulations of other Members.[93]

The U.S. NIST or another cybersecurity standard-setting agency could engage in similar efforts in connection with low risk IoT. Obviously, recognition or equivalence would be easiest in the cybersecurity area (as it is in the food safety field) with trusted countries, such as the "Five Eyes"—Australia, Canada, New Zealand, the U.S., and the U.K., that share similar regulatory philosophies, standards of protection, and security goals. However, given the amount of trade that could be at stake, other countries may seek to provide reliable regulatory regimes, and appropriate assurances, that their low risk IoT is safe enough to accept.

---

[91] SPS Agreement, Art. 4.

[92] U.S. Food and Drug Administration, International Cooperation, page last updated October 4, 2018, available at https://www.fda.gov/Food/InternationalInteragencyCoordination/InternationalCooperation/default.htm.

[93] TBT Agreement, Article 2.7.

A fourth method of international cooperation utilized by the U.S. FDA, involving on-site verification, may assist in providing sufficient assurances. Under the 2011 Food Safety Modernization Act (FSMA), the FDA maintains a foreign inspection program to "ensure the U.S. food supply is safe by shifting the focus from responding to contamination to preventing it."[94] While physical inspection of a foreign food processing plant is quite different from inspection of software compilation or other aspects of IoT cybersecurity, some aspects may be analogous, such as the ability to audit the system for production in order to ensure that the software installed is identical to the software inspected. A system along the lines of the U.K.'s HCSEC utilized with Huawei for network equipment could be used, perhaps with somewhat less rigor, in connection with low risk IoT. The core question is the extent to which observation of production, or analysis of products, can assure the security of IoT products.

ii. Sarbanes-Oxley, Foreign Private Issuers, and Overseas Audit

Under the Sarbanes-Oxley Act of 2002 (Sarbox), companies that wish to have their securities traded in U.S. capital markets, public companies, including foreign companies, must periodically file audited financial statements with the U.S. Securities and Exchange Commission (SEC). Under Sarbox, the auditor of those financial statements must be registered with, and therefore subject to the jurisdiction of, the Public Company Accounting Oversight Board (PCAOB). Registered auditors must undergo regular PCAOB inspections to assess their compliance with relevant U.S. law and professional standards. While some countries, including China, have rejected this "extraterritorial" inspection regime, it serves as a potential model for an IoT cybersecurity regime. The core question, of course, as discussed above in connection with the FDA foreign inspection program, is the extent to which security of IoT products can be ensured by on-site inspections.

iii. Policy Options

Subject to a determination that a particular IoT product is within the low risk IoT category (and recognizing that more precise distinctions may become necessary), it is not difficult to identify a path toward maintaining free trade while preserving sufficient levels of cybersecurity.

1. Trade

In the trade context, each state will specify its own "appropriate level of protection" for different forms of low risk IoT, and then the SPS model of harmonization, equivalence, and mutual recognition, including possibly harmonization, equivalence, mutual recognition, and foreign inspections. The SPS Agreement, and action thereunder, provides a useful model for combining these techniques of combining free trade and protection goals. Because these techniques have been shown to provide adequate policy space for security in connection with disease-causing agents and contaminants in food, here is no need to utilize security exceptions, and they should be recognized as being as inapplicable in low risk IoT as they are in the SPS field.

[94] U.S. FDA, Foreign Food Facility Inspection Program Questions & Answers, last updated September 19, 2018, available at https://www.fda.gov/Food/ComplianceEnforcement/Inspections/ucm211823.htm.

2. Investment

With respect to investment, the same types of regulation and international cooperation techniques can sufficiently ameliorate risk, made easier by the fact that investment in a host country is more readily understood as under the territorial regulatory jurisdiction of the host country.

b. High Risk IoT: Trust or Verify

The obstacle to trade in high risk IoT goods is that, by definition, a very high degree of confidence of safety is required. This confidence can only be supported by high levels of trust or high levels of verification.

While trust is often associated with nationality, or at least nationality of beneficial ownership and control, of the producer, this basis for trust must look inside the producer to evaluate the trustworthiness of its supply chain and employees. Furthermore, if production or other relevant activities take place outside the territorial jurisdiction of the consuming state, then the cooperation of the producing state must be examined as well. Thus, even production within one of the five eyes states is not sufficient assurance of security.

Therefore, trust can only be established by a detailed due diligence analysis of the persons involved at all phases of production that present vulnerabilities.

For high risk IoT, verification may vary depending on the degree to which trust is established. But verification will involve assessment of the vulnerability of the software and hardware comprising the IoT product, including vulnerability to hacking by third parties.

States will be reluctant to give up the flexibility of the security exception, to allow them to block imports of, or investment in production of, high risk IoT goods entirely, or when produced by manufacturers that, in the importing state's view, do not sufficiently merit trust. Under these circumstances of high risk and low trust, strong verification is the only basis for trade or investment.

i. A Globalized HCSEC Model

The British government's HCSEC structure, discussed in Part 1 above, represents one attempt to provide for independent, competent, verification of relevant products. While the HCSEC oversight board has found difficulties in determining that the software inspected is the same as the software installed, and there may be other technical limits that make verification for goods manufactured by a producer that is accorded a low level of trust impossible, further evaluation will be necessary to determine whether satisfactory verification is possible. If it is, then from the manufacturer's standpoint, it would be desirable to have a global approach, with a single body charged with verifying the safety of high risk IoT products for the global market.

A globalized HCSEC model might include harmonized security standards and globally agreed verification procedures, as well as globally agreed assurances of independence. The

International Atomic Energy Agency, discussed below, includes some features worth considering.

ii. The International Atomic Energy Agency Safeguards Model

Under the Nuclear Non-Proliferation Treaty (NPT), member non-nuclear-weapon states commit not to acquire nuclear weapons, and to accept International Atomic Energy Agency (IAEA) safeguards on civilian nuclear material to verify compliance.

> At the technical level, safeguards comprise procedures and measures to detect, identify, characterize, and quantify nuclear material, and to assess the significance of nuclear activities. An international inspectorate, the IAEA, applies these procedures and measures with the cooperation—in theory and in the vast majority of cases in practice—of national authorities.[95]

Of course, IAEA safeguards have failed to detect nuclear weapons programs on several occasions. The question worth evaluating is whether the IAEA safeguards model can suggest features of an international safeguards regime for high risk IoT production.

iii. Policy Options

For both trade and investment, high risk IoT will require strong verification techniques, applied at the time of production as well as at the time of any updates. Strong verification will be costly, but harmonization of standards and centralization of verification, or perhaps a more limited regime of recognition, will ameliorate the costs.

6. Conclusions

Trade and investment in low risk IoT products will be manageable along traditional lines of other product standards (analogously to the EU's GDPR), regulated by the GATT and TBT Agreement to assure national treatment, MFN treatment, proportionality, and due respect for international standards. With respect to high risk IoT products, the path to efficient trade and investment is less clear, and will depend on the technical ability to surveil and confirm the safety of IoT products. It will be difficult to rely on trusted suppliers, whether on the basis of nationality or territoriality, because of the complexity of production and the magnitude of risk. States will restrict imports and investment in high risk IoT products under security exceptions in trade and investment law, although the language of those exceptions do not necessarily support such restrictions. In some circumstances, restrictions will be based on protectionism or geoeconomic considerations, rather than cybersecurity per se. States will find it useful to identify means to verify security of high risk IoT products, and to establish trust in producers of IoT products, and on the basis of sufficient combinations of verification and trust, to relax or constrain their use of security exceptions.

---

[95] John Carlson, Future Directions in IAEA Safeguards, Belfer Center Discussion Paper, November 2018, available at https://www.belfercenter.org/publication/future-directions-iaea-safeguards.