Center for Technology Innovation at BROOKINGS

September 2013

Cybersecurity and Trade:
National Policies, Global and Local Consequences

Allan A. Friedman

Allan A. Friedman
is a fellow in Governance Studies and research director of the Center for Technology Innovation at the Brookings Institution.

INTRODUCTION

In 2009, the Centre for Economic Policy Research published a 100-page collection of essays on the rise of trade barriers and "murky protectionism" following the financial crisis.[1] The word "technology" appears only once in that report. Information technology has often been seen as a huge success story in global trade, but its rapid diffusion has introduced new risks. Modern economies, developed and developing, are increasingly reliant on their IT-supported infrastructure for almost every aspect of daily life. Yet, as the headlines attest, this infrastructure is less than perfectly secure, and the rapidly evolving threat landscape exposes the dependent societies to dramatic risks. The interdependence of systems and institutions means that a security failure can have dire consequences.

Governments around the world have begun to develop strategies to protect themselves against cyber threats while trying to promote the benefits of a cyber-enabled world. NATO's Cooperative Cyber Defense Center of Excellence has identified over 50 countries that have published a cybersecurity strategy "defining what security means to their future national and economic security initiatives."[2] Scholars have identified common themes across most declared strategies, indicating that the generalized risks faced by all of us are not that different.[3]

1 Baldwin, Richard, and Simon Evenett. *The Collapse of Global Trade, Murky Protectionism and the Crisis: Recommendations for the G20*. CEPR (2009).

2 Klimberg, Alexander (ed). "National Cyber Security Framework Manual." NATO CCD COE Publications. (December 2012). http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

3 Organisation for Economic Co-operation and Development. Cybersecurity Policy Making at a Turning Point. (2012). http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

It is one thing to propose broad goals. It is another to work towards enacting these strategies. It is the policies that fulfill these strategic goals that will shape the digital future, defining cyberspace not just for the countries themselves, but the broader globalized Internet society. As countries begin to implement policy and "the focused application of specific governmental levers and information assurance principles,"[4] the differences can inform us about what works and what does not.

Perhaps equally important, studying cybersecurity policies can help us understand the secondary consequences of seeking a more secure cyberspace. This paper will survey the nascent but burgeoning area of cybersecurity policy and identify how public policies will interact with the private provision of the IT products they seek to regulate. In particular, how do cybersecurity policies affect the globalized trade of information technology and the growth and development these technologies have promised?

After reviewing the arguments for government involvement in securing information systems, this paper will review different types of initiatives that have emerged from countries around the world, and explore their potential impact on improving security. In addition to their impact on risks, some government actions can distort the market for IT goods and services. The second half of this paper examines the economic impact of security-motivated policies that serve as barriers to trade. Given the magnitude and importance of the topic, I lay the foundation for a larger research agenda, and offer a set of policy recommendations for governments and IT stakeholders.

THE ROLE OF GOVERNMENT

The threats are vivid, and require the attention of any government that seeks to safeguard the security and stability of its citizens. The protection of lives and property from foreign actors is a universally understood role of government, and the cyber era introduces new capacities for other nations to wage war. As cyberlaw theorist Paul Rosenzweig points out, just as everyone would expect the government to defend against enemy aircraft rather than leaving it to each individual or enterprise, so too would we expect the imperative of "the common defense" to extend into cyberspace.[5] This also includes the threat of non-state actors targeting civilian infrastructure for political gain, even if the threat of cyberterrorism is perhaps overstated.[6] Governments have also grown every bit as dependent on information technology as the rest of us, and political adversaries seek to learn others' state secrets and gain a strategic advantage by compromising the systems that hold valuable state secrets.

4 Klimberg 2012.

5 Rosenzweig, Paul. "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence." Deterring Cyberattacks: Informing Strategies and Developing Options, *National Research Council* (Forthcoming 2010).

6 Singer, Peter and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. (Forthcoming 2014).

The role of government spills over into more mundane motives such as profit. Just as governments seek to enforce intellectual property rights of their citizens to promote innovation through patents and international trade negotiations, they must protect their industries from cyber theft of competitive data.[7] Criminals have also learned that the new digital domain offers new opportunities to exploit consumers and businesses alike. This triggers a traditional state interest in law enforcement and crime prevention. More generally, any government that wishes to promote the growth of its digital economy will seek to foster trust in the digital systems that underpin the information ecosystem.

This ecosystem, or the "critical information infrastructures" are either critical infrastructures themselves, or are necessary for the operation of critical infrastructure. Defining "critical infrastructure" is itself political and depends on national policies and priorities, but for the purposes of this paper, the United Kingdom's definition should suffice: that which "supports the economic, political and social life" of the country, and whose failure could cause "large scale loss of life, have a serious impact on the national economy, have other grave social consequences for the community or, be of immediate concern to the national government."[8] The focus here is on the public interest, and threats that could affect the whole of society. As others have noted, what makes this particularly thorny for government action is that most of this infrastructure is privately held and managed. The networks themselves are run by private enterprises throughout most of the world, and many of the systems on which we depend that use the network—electricity, transportation, etc—are also run by private enterprises.

What can governments do? There are many broad and slightly "fuzzy" roles for state leadership in cybersecurity. They must coordinate different efforts, manage stakeholder interests, and educate the populace to establish cybersecurity as a priority. This can be incredibly effective, but ultimately the case might be made for stronger government intervention through policies and regulations.

More than a few cybersecurity experts and industry representatives have argued that cybersecurity regulation, in general, will do more harm than good. The United States Chamber of Commerce, for example, argues that, "regulators may not move fast enough to keep up with the dynamic cyber threat, and if businesses focus only on meeting government standards, they will be hard pressed to address new and changing cyber realities."[9]

7 Friedman, Allan. "Cyber Theft of Competitive Data: Asking the Right Questions." The Brookings Institution. (Forthcoming 2013).

8 Organisation for Economic Co-operation and Development. "Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security." (2008) http://www.oecd.org/daf/inv/investment-policy/40700392.pdf

9 U.S. Chamber of Commerce. "Cybersecurity: More Government Regulation?" (2012) http://www.uschamber.com/feed/cybersecurity-more-government-regulation

This paper does not explicitly argue for or against the need for new cybersecurity regulation. Instead, it acknowledges that a sufficient number of cybersecurity experts and policymakers around the world believe that cybersecurity regulation will be necessary, and seeks to understand the impact. Moreover, while others have linked IT trade and values such as Internet freedom[10], that is also outside the scope of this study.

Why do some feel that government intervention is necessary? Intervention advocates point to the widespread lack of good information security, and see that since the privately-held infrastructure has failed to secure itself, the government must step in. Several theoretical points are held up to explain the failure of the market. First, infrastructure providers may lack direct incentives to invest in costly security measures if they will not be held fully accountable for preventable failures. Second, the interdependence between the subsystems, components and function-specific equipment and contexts makes it hard to hold any one person responsible. Finally, the market currently lacks clear signals about security quality, making it difficult for an interested infrastructure provider to know that their investment was effective.

CYBERSECURITY POLICIES – INTENTIONS AND EFFECTS

GOVERNMENT PROCUREMENT REQUIREMENTS

It is natural for governments to begin thinking about cybersecurity by trying to get their own house in order. Not only is this much easier to do through most policy processes than private sector regulation, but states have a strong interest in securing their own systems. There is an understandable concern over the confidentiality and integrity of government data. Mandates for security systems often take the form of procurement requirements and regulations. In most countries the government, and the agencies it controls, are together the biggest purchasers of goods of all kinds, ranging from basic commodities to high-technology equipment. With this sizeable budget, governments can often use their purchasing power to push for specific technical goals to improve government systems, for everything from improved power consumption to standardized interfaces.

Many governments have proposed security standards or requirements for their purchasing systems. The efficacy of these policies has been mixed. On one hand, they are undoubtedly better than the alternative of traditional lowest-bidder deals that give government IT systems a poor reputation. On the other hand, the sheer size of most national or even local bureaucracies, combined with the lumbering pace of acquisition and replacement cycles makes management and enforcement of these policies slow and costly.

From a trade perspective, large government contracts can help define standards and build out a large platform for future innovation. At the same time, the political pressure to

10 Aaronson, Susan. "Trade and the Internet." *The International Economy* (2012): 75.

favor domestic suppliers over their foreign competitors can be very strong. This has been recognized as a potential barrier to trade. An Agreement on Government Procurement (GPA) was negotiated in the World Trade Organization (WTO) and went into effect in 1996, setting out principles of "openness, transparency and non-discrimination" for the signatories' national and local procurement processes.[11] This does not apply to the whole WTO membership: only the European Union, the United States, Japan, Korea and a handful of other countries have signed it.

It is easy to see how the procurement process might impact the free flow of goods, whether intentionally or otherwise. Government purchasing requirements are notoriously complex. In the U.S., there are regular calls to reform the mass of red tape that requires extensive experience to master. There is practically no standardization across countries, such that the process to certify as secure for one country—say, America's Federal Information Security Management Act (FISMA)—would require a completely different set of certifications than those to meet Japan's Information Security Policy Council (ISPC) standards.

Beyond these normal bureaucratic hurdles, countries have begun to impose more specific requirements or regulations for government procurement. Canada, which is a signatory to the WTO's GPA, recently declared a bidding process to consolidate the government's many non-interoperable email platforms into a single system. They introduced several measures that could be seen as discriminatory, including limiting bids to Canadian firms, or Canadian subsidiaries, and requiring that support personal must be Canadian citizens. The country recognized that this does not conform with the GPA, but insisted that the national priority is "to create a secure, centralized communications infrastructure," and thus it invoked the National Security Exception to its trade agreements.[12] It's important to note that the email system Canada is building is *not* for "top secret" data.

If limiting all foreign participation in government system might fall within the bounds of a national security priority, what about explicitly forbidding components from a single country? The United States Congress declared that four government agencies, including the Departments of Commerce and Justice, could not buy "information technology systems" that were "produced, manufactured or assembled" by entities "owned, directed, or subsidized by the People's Republic of China" unless the head of the purchasing agency consults with the FBI and determines that the purchase is "in the national interest of the United States."[13]

11 World Trade Organization. "Plurilateral Agreement on Government Procurement." (2011) http://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm

12 Shared Services Canada. "Statement on cybersecurity." October 9, 2012. http://www.ssc-spc.gc.ca/pages/news-nouvelles-eng.html

13 United States Congress "Consolidated and Further Continuing Appropriations Act" 2013. http://www.gpo.gov/fdsys/pkg/BILLS-113hr933enr/pdf/BILLS-113hr933enr.pdf

NATIONAL SECURITY STANDARDS

Beyond the systems used by the government itself, governments have also begun to see a state interest in ensuring that the IT systems used by their citizens are secure, particularly in their critical infrastructure. As mentioned above, this is often motivated by the belief that market actors will not invest in security themselves, either through demand or supply-side failures. Governments can encourage or require those who safeguard data and digitally supported services to better protect their systems.

Policy options range in both the type of standard, and the process by which standards are promoted and promulgated. In the United States, initial attempts to establish greater legal authority to promote standards failed to gain sufficient support in Congress. Subsequently, the Administration proposed a Cybersecurity Framework (CSF) "of standards, guidelines, and best practices to promote the protection of critical infrastructure." The National Institute of Standards and Technology (NIST) drafted this Framework after an intensive period of consultation and engagement with stakeholders from industry, academia and government. A preliminary discussion draft was released in August of 2013.[14]

The CSF has two unique features from the perspective of government standards policy. First, it is voluntary, and the government has sought, in parallel, to explore how to promote compliance through incentives. Second, as of the fall of 2013, the initial draft did not specify any new standards or paths towards assurance, but reviewed and compiled existing standards and best practices. This has led to criticisms that the CSF would not be effective. Industrial Control Systems expert Ralph Langner complained that the "application of the CSF has no predictable effect on empirical system properties." Part of the problem, he notes, is the lack of stricter standards. "The CSF allows any organization, no matter how good or bad at cyber security, to be CSF-conformant."[15]

China, on the other hand, has proposed a more expansive set of policies with more explicit security requirements not just of the technology, but of the process itself. These measures define different levels of protection requirements, and are commonly referred to in English as the Multi-Layer Protection Scheme or MLPS. (China scholar Nathaniel Ahrens notes that a Chinese WTO representative stated that the measure should be referred to as the Regulation on Classified Protection of Information Security,[16] but almost every other English language

14 National Institute of Standards. "Discussion Draft of the Preliminary Cybersecurity Framework." (August 28, 2013). http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf

15 Langner, Ralph. "What a Cybersecurity Framework for Industrial Control Systems Needs to Look Like." (September 4, 2013). http://www.langner.com/en/2013/09/04/what-a-cyber-security-framework-for-industrial-control-systems-needs-to-look-like/

16 Ahrens, Nathaniel. "National Security and China's information security standards" CSIS Hills Program on Governance. (2012). https://csis.org/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf

reference uses the term MLPS.) These policies define the importance of certain infrastructures, and the protections required for different levels.

Schema that define different security classifications are not uncommon. NIST's 800-63 guideline on authentication, for example, uses different "levels of assurance" depending on the context.[17] The security policy challenge is in defining these levels to provide appropriate levels of security for the risk. Since its introduction in 2007, the MLPS has drawn fire for how it defines sensitive networks, and certain requirements of those sensitive networks. Of the five levels, the policy requires that any instance where damages will harm national security, social order, economic development or public interest be governed by Level III protection or "supervised protection."[18] This definition does not clash aggressively with other countries' definitions of critical infrastructure, but it does include most major industries in China, from finance to health care.

The critical information infrastructure regulations include some general certification requirements, such as a yearly certification process, and an attestation that the systems do not have security flaws. Beyond these, however, the regulations have drawn extensive criticism for legal requirements of domestic ownership of both the technology vendor and the underlying intellectual property rights of the product. This goes a step beyond the procurement requirements discussed above to essentially dictate national control for an entire market. This can set up long-term barriers in everything from finance to health care services if the provisions give a natural, lock-in advantage to domestic providers. How would this make a country more secure? In theory, this mitigates the risk of a foreign vendor refusing to secure or harden critical information systems, or is not fully trusted to do so. Domestic ownership requirements could potentially give the country and its domestic industrial capacity the ability to safeguard themselves. However, this threat must be balanced against the reality that such a requirement effectively locks out foreign IT vendors from most major industrial sectors, running counter to the general principles of free trade.

TESTING AND CERTIFICATION

Even when governments do not impose a specific set of security requirements for information systems, they may still have an interest in verifying that the products sold in their domestic markets are secure. Testing can be expensive, complicated and vary by the security goals as well as methodological approaches to risk.

Until the late 1990's, there were few international approaches to certifying security assertions, particularly for very sensitive applications inside the national security community. To enable

17 National Institute of Standards and Technology. *NIST Special Publication 800-63 Version 1.0.2*. Washington. (2006).

18 Ministry of Public Safety. "Classification Guide for Classified Protection of Information System Security." (2008). (Translated by Jing Ran)

coordination of their various assurance efforts, the United States, the United Kingdom, Canada, France and Germany unified their standards process in 1998, creating the Common Criteria. Joined by the European Union and a handful of other countries, the Common Criteria allows for context-specific evaluation of key goods by matching security requirements to security assertions in a fashion that can be verified by independent testing labs.

Of course, this process can be very expensive and time-intensive, especially for higher levels of security. Independent testing can introduce perverse incentives if testing labs compete to win business of those who wish to pass a certification process.[19] Yet other methods can be even more onerous. Even if they are more efficient, if different countries propose separate certification procedures, that can add costs and delays to the time to market, particularly if the certifying institutions don't follow international norms of product evaluations. To address concerns of the UK security officials, for example, a Chinese IT vendor funded an independent lab to certify that their products were secure through an independent process.

To fully trust that a piece of software or hardware does what it claims to do, a country may be tempted to demand full access not just to the product, but the underlying source code, architecture and intellectual property. Brazil's National Broadband Plan originally included a provision in the public contract for access to source code, and China's initial Compulsory Certification Program both initially required foreign vendors make their source code available to assure adequate security, although these proposals were later walked back.

ENCRYPTION

From its use to protect state secrets, encryption has evolved to become ubiquitous in every day ICT products. Beyond ensuring confidentiality, modern commercial cryptography now protects the integrity of everything from online identity to electronic car door locks. Given its historical links to military use, encryption has in the past been regulated to a certain extent. For instance, the U.S. government classified encryption products as "munitions" and subjected them to strict export controls until the 1990's.

With the development of easy-to-use encryption technology and the spread of the Internet and e-commerce, which dramatically increased demand for encryption, such restrictions came to be seen as causing more harm than benefit. After a protracted policy battle, the Clinton Administration dropped plans to impose unwieldy regulations on such products and removed most restrictions on exports, leading to a widespread trend towards similar deregulation elsewhere. Cryptography is now a basic feature in a huge range of information systems, primarily based on open, international standards.

19 Anderson, Ross. "Why information security is hard-an economic perspective." *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*. IEEE. (2001).

Still, several countries have identified security risks in using cryptographic systems without further government supervision. Why a particular focus on regulating cryptography? From a cybersecurity perspective, the state could distrust the available technology as providing insufficient security for the needs of the country and its interests. Alternatively, the government could feel that encryption standards are too strong, and hinder its ability to defend the national interests through surveillance, under the rubric of "information security."

If states fear that underlying technology is not trustworthy, they may demand a special certification process for cryptographic technology, or even stronger policies. Russia has had extensive national licensing requirement for any encryption-related technologies. Although the government has pledged to work with the international community to streamline the process and make the certification process easier, many vendors continue to report an onerous ad hoc process with minimal transparency. Other countries go further, demanding code or even proposing their own. For example, in the 2000's, Korea had a short-lived requirement for the disclosure of source code for information security products sold to the government. States may also push for their own standards, such as the Chinese advocacy of the WAPI wireless standard or Korea's push for domestic VOIP standards.

Regarding concerns about information security for domestic security, we might expect to see bans or limits on the use of foreign cryptographic technology, such as Vietnam's proposed 2013 law. In 2012, India proposed a Policy for Providing Preference to Domestically Manufactured Electronic Goods (PMA) that privileges domestic telecommunications manufacturers for both public and private sector purchasing, including IP-based encryption products.[20] (This policy is currently on hold pending domestic review).[21] Chinese policies on the use of foreign cryptography in some applications have actually limited the use of standardized transport-layer security by Chinese web companies, denying even basic password protection. Evaluating these approaches as security policies becomes difficult, because the goal of "security" becomes less obvious. While some countries such as the United States can maintain intelligence by obtaining encryption keys, others may not have that advantage. Meanwhile, the rejection of international cryptographic standards may not be as crazy as they had appeared. Recent disclosures about American interference in an internationally recognized cryptographic standard shocked the security community, and spread concern about the stability of other global standards.[22]

20 Ministry of Communications and Information Technology. "Notification on Policy for Preference to Domestically Manufactured Telecom Product." (October 2012). http://www.dot.gov.in/sites/default/files/5-10-12.PDF

21 "Govt to review 'preferential market access' policy that gave opportunity to domestic manufacturing." *India Times*. (July 8, 2013). http://articles.economictimes.indiatimes.com/2013-07-08/news/40443725_1_pma-policy-preferential-market-access-policy-private-sector

22 Perlroth, Nicole, Jeff Larson and Scott Shane. "N.S.A. Able to Foil Basic Safeguards of Privacy on Web" *The New York Times*. (September 5, 2013). http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0

ECONOMIC IMPACT OF CYBERSECURITY-RELATED TRADE BARRIERS

If the policies described impede the global flow of IT products and services, there could be economic impacts not only to the IT firms and vendors, but the importing countries as well. The consequences would depend on the policies. Some offer a large enough trade barrier to substantially deny market access, while others may raise the costs of production and thus the costs of the consumer in the importing country.

NATIONAL SECURITY EXCEPTIONS

International trade agreements promote the global flow of goods and services by binding countries to rules minimizing trade barriers. Yet going back to the beginning of the modern globalized trade era in 1947, the General Agreement on Tariffs and Trade was built on an understanding that trade could not pre-empt a country's ability to defend itself. Article XXI states that "nothing in this Agreement shall be construed... (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests." Just how strong this and a handful of other related trade agreement national security exceptions are has generated some debate,[23] but a key point emerges: a unilateral declaration of national security interest could be sufficient to remove trade agreement obligations with minimal recourse.[24]

Actual invocation of these rights has been incredibly rare, and a full legal challenge has never occurred. Part of this is due to the rarity of trade and security conflicting, but it is also because unilateral declarations of this kind would set a terrible precedent. It would invite others to respond in kind, removing the affected goods or sectors from the entire trade arrangement. This 'mutually assured destruction' approach has helped restrain WTO members in the past, but this only makes any invocation even more dangerous. Not only would it inspire retaliation, but make it easier for others to use in the future.

Trade law expert Raj Bhala notes that the language offers some protection by requiring that these actions are "necessary" for the "protection" of that member's "essential security interests."[25] In many cases, this would help serve as a check against invoking XXI for, say, mineral exports. In the context of critical information infrastructure protection, however, the lines are far less clear.

Nathaniel Ahrens argues that we can read broader checks in the surrounding language that explicitly references direct or indirect support of a military establishment, and that these

23 Lindsay, Peter. "The ambiguity of GATT article XXI: Subtle success or rampant failure?" *Duke Law Journal* 52.6 (2003): 1277-1313.

24 Bhala, Raj. "National Security and International Trade Law: What the GATT Says, and What the United States Does." *University of Pennsylvania Journal of International Law*. 19 (1998): 263.

25 ibid

actions are only valid "in time of war or other emergency in international relations."[26] Yet this language is also filled with ambiguity. As Ahrens acknowledges, a country could point to the cyber attacks against Iran's nuclear program as potential justification for invoking a national security environment.

The economic consequences of ignoring free trade obligations to protect critical infrastructure could be devastating. If the country invoking it has a substantial export sector, then their own economy would suffer greatly if their trade partners invoked the exception in retaliation This mutually-assured destruction game has kept WTO members in check thus far, and makes this a huge first threshold. The real risks are the sheer scope of goods and services that might fall under such an action. As Darrell West points out, the supply chain for information technology is global.[27] IT products are, in turn, deeply embedded in the critical infrastructure, implying a cascading failure that could deprive everyone of IT goods following a single invocation.

FOREIGN DIRECT INVESTMENT AND INTELLECTUAL PROPERTY POLICIES

Some of the policies discussed above do not pose the same potential for a global chain reaction of trade disruption, but can still serve to disrupt the flow of IT goods and services around the world. Bans on foreign direct investment and sales will remove firms or entire classes or products from domestic markets. Mandatory intellectual property disclosure may serve the same purpose if companies choose to exit particular markets, or choose not to enter them. Free trade, while not without controversy, has been shown to foster development, growth and innovation.[28] The issues surrounding cybersecurity regulation may raise the stakes because of the particular dangers of protectionism in the IT sector.

Hwan-Joo Seo et al found found a positive relationship between IT investment and economic growth in both wealthy OECD countries and developing countries.[29] Hopeton S. Dunn finds particular benefits in the Caribbean, and makes the case of IT trade and development: "Though not without its critics, the general consensus is that reducing trade barriers for ICT has an overall positive impact."[30] This argument that IT investment works best when accompanied by

26 Ahrens, Nathaniel. "National Security and China's Information Security Standards" CSIS Hills Program on Governance. (2012).

27 West, Darrell. "Twelve Ways to Build Trust in the ICT Global Supply Chain." Issues in Technology Innovation. (2013). http://www.brookings.edu/research/papers/2013/04/18-global-supply-chain-west

28 Kiriyama, N. (2012), "Trade and Innovation: Synthesis Report," OECD Trade Policy Papers, No. 135, OECD Publishing. http://dx.doi.org/10.1787/5k9gwprtbtxn-en

29 Seo, Hwan-Joo, Young Soo Lee, and Jeong Hun Oh. "Does ICT investment widen the growth gap?" *Telecommunications Policy* 33.8 (2009): 422-431.

30 Dunn, Hopeton S. "ICT Policymaking and International Trade Agreements in the Caribbean." *The Handbook of Global Media and Communication Policy*. (2011): 395.

a more open trade stance in that sector is borne out in cases as diverse as Central America[31] and Southeast Asia.[32]

Information technology is recognized as being particularly important for growth and innovation because it forms an integral component to so many aspects of the economy. During the 1990's, economies gained more from using information technology than they did from the production and sale of these technologies.[33] Given the evident benefits of IT consumption, when IT industry proposed a liberalization of trade for IT products, they found ample support from the world trade community. The result was the Information Technology Agreement (ITA) an agreement between a subset of WTO members, 78 as of 2013, to bring tariffs on IT down to zero. The ITA offers some of the best evidence of the benefits of open global trade of IT products. While it is hard to separate out the growth of the IT sector from the impact of reduced tariffs, Bora and Liu find that joining the ITA increases IT imports.[34] This makes sense: lower tariffs promote IT imports, further feeding the economy and the use of networked technology. While no research has quantitatively linked imports with IT use in the local economy, it seems a natural progression.

Erecting trade barriers to limit the players in a local market has many of the same consequences as traditional tariffs—albeit much harder to measure. If anything, keeping foreign competition out of the market will have a more direct impact: lowered competition raises costs for consumers, and can reduce pressures on innovation. Even when policies are only directed at a smaller set of exporters, rather than closing the market against all players, competition can suffer. For IT markets that are not perfect commodities, strategies such as bundling and cross-compatibility enable customers to maximize the value of their IT investment. When certain vendors cannot play, the game is distorted.

Cybersecurity policies such as targeting foreign firms don't just close the market to imports, they have been used to limit foreign direct investment, discouraging international firms from developing local partnerships. These partnerships lead to the diffusion of knowledge and productivity increases, through spillovers with partners, suppliers and the local labor market.[35] The larger partners, in return, gain access to a cheaper labor supply, and tighter links to

31 Villalobos, Vilma and Ricardo Monge-González. (2011). Costa Rica's Efforts "Toward an Innovation-Driven Economy: The Role of the ICT Sector." *The Global Information Technology Report*. San Jose: World Economic Forum. (2011). https://reports.weforum.org/wp-content/pdf/gitr-2011/03-part-2/2.1-costa-ricas.pdf

32 Irawan, Tony. "ICT and economic development: comparing ASEAN member states." *International Economics and Economic Policy*. (2013): 1-18. APA.

33 Kraemer, Kenneth L., and Jason Dedrick. "Information technology in Southeast Asia: engine of growth or digital divide?" *Information Technology in Asia: New Development Paradigms*. (2002).

34 Bora, Bijit, and Xueping Liu. *Evaluating the impact of the WTO Information Technology Agreement*. WTO Working Paper. (2006).

35 Keller, Wolfgang. *International trade, foreign direct investment, and technology spillovers*. No. w15442. National Bureau of Economic Research, 2009.

new markets. Of course, at the extreme, policies that require IP transfers or disclosure will discourage direct investment by introducing new costs in terms of potential market threats. Finally, while the "illicit technology transfer" that can occur when competitive data is stolen from a corporate partner does not meet the definition of a cybersecurity policy, it will have a similar effect. In countries when a joint venture may mean the theft of competitive data, partnering firms will at the very least be forced to pay for added data protection, and may lose the trust of their local or international partners.

TECHNICAL STANDARDS

Other proposals and policies discussed above don't deny market entry, but they do raise the costs. Some technical features do better serve the market if their legal imposition addresses a market failure, but all requirements do distort the market through added costs. Complying with technical standards can add extra steps and expenses to the production process, and demonstrating compliance can delay products reaching the market. This does not itself imply that standards are a trade barrier. Rather, when these standards "either (i) create a wedge between domestic and foreign prices or (ii) affect trade flows," they become a non-tariff barrier (NTB) to trade.[36] Many attempts to document NTBs in the WTO era have found that a huge percentage, if not a majority, of traded goods are affected by NTBs. Further, technical standards have become the most prevalent NTB—surpassing other measures such as subsidies—and are reported to be the most difficult to comply with.

Some argue that technical standard requirements are less draconian than traditional trade barriers. Nevertheless, these requirements may have large impacts on global trade. Timeliness is critical for the IT sector, particularly as markets and governments clamor for more secure solutions. They are also one of the most natural tools for a more well-intentioned moderate policymaker who is aware of the larger trade issues of outright import bans. If policymakers are concerned about IT, sourced domestically or internationally, standards and technical requirements might make sense.

As noted above, the origin of these standards can make a difference. Universally accepted international standards can still substantially impact trade, particularly for agricultural goods where poorer countries may not have the resources to comply. Information technology, however, is built on standards for interoperability, so producers assume some baseline of compliance. Things get much more difficult when dealing with nation-specific standards. Bespoke technical standards disrupt the global market by fragmenting it. Economies of scale allow vendors to export one product globally. When importers demand specific properties, this can dramatically raise the cost of production. IT products are extensively tested for reliability,

36 Olivier Cadot, Sebastian Saez, and Maryla Maliszewska. "Non-Tariff Measures: Impact, Regulation, and Trade Facilitation" *Modernizing Border Management*; Washington. Ed. Gerard McLinden. Washington, DC: The World Bank, 2010.

compatibility and, yes, security. Each fork in the standards environment doubles the workload. It also increases support costs, and many other economies of scale in the IT industry. A globally accepted standard can dramatically increase innovation by providing a global platform on which to build. The story of the IT industry is the story of successful standards that have allowed innovators to build new tools, features or applications that can compete on top of the standardized platform.

Technical standards as NTBs have been of great interest to researchers, but have proven particularly difficult to study because of the heterogeneity across different sectors. A recent study of all traded goods found that announcing a new standard reduces the probability of exporting to that country, but also identified instances where standards could increase trade.[37] One of the few papers to look at high-tech trade found that Europe's internationally harmonized electronics standards increased imports to the EU significantly.[38] Harmonization made trade easier. Another study found that goods with long and complex supply chains—common to many IT goods—were more likely to be negatively affected by imposed standards.[39]

On the other hand, other work found that technical standards could actually increase trade, even when adopted at a national level.[40] One common theory was that standards provide a signal of quality, increasing trust and thus demand. This resonates with the cybersecurity story in terms of demanding trust, but does not fit well in the context of a globally standardized IT ecosystem.

FURTHER RESEARCH QUESTIONS

It is critical to understand whether and how cybersecurity regulations will actually introduce harms in terms of economic growth and trade. As noted above, the general understanding of information technology trade and barriers to that trade is far from complete. Researchers are held back by a lack of data and precise models.

Yet as governments explore their cybersecurity policy options, it is imperative to understand the distinctions between the primary impact of increasing security and the secondary order effects on trade. It is entirely possible that trade-offs exist between security and efficiency,

37 Bao, Xiaohua, and Larry D. Qiu. "How Do Technical Barriers to Trade Influence Trade?." *Review of International Economics* 20.4 (2012): 691-706.

38 Portugal-Perez, Alberto, JoséÐDaniel Reyes, and John S. Wilson. "Beyond the Information Technology Agreement: Harmonisation of Standards and Trade in Electronics." *The World Economy* 33.12. (2010): 1870-1897.

39 Ferrantino, Michael. "Using supply chain analysis to examine the costs of non-tariff measures (NTMs) and the benefits of trade facilitation." (2012). Staff Working Paper ERSD. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1988245.

40 Marette, Stéphan, and John Beghin. "Are standards always protectionist?." *Review of International Economics* 18.1.(2010): 179-192.

imposing some loss on domestic economies in exchange for less systematic risk to our critical information infrastructures. This is separate from any negative externalities that these regulations could inflict on the global economy through interruptions in the flow of information and information technology. Below are some key questions that would inform this international debate.

Heterogeneous costs of compliance. Technical standards can actually be anti-protectionist if foreign producers are more efficient at addressing these risks. For any given security standard, different producers may approach them differently, incurring different costs. Can we expect security standards, either international or domestic, to drive innovation? Would different approaches to developing security regulations lead to a more thorough search for security solutions?

Supporting local innovation. As noted above, social and institutional conditions play a major role in mediating the effect of IT on development projects and goals. Many instances of success turn on an understanding of how to adapt and implement information systems for the immediate context, rather than turnkey solutions. How do trade barriers or their absence affect local capacity for innovation?

Risk as a trade barrier. Standards trade theory says that technical standards can increase access to export markets by informing customers and addressing information asymmetries. Absent functional standards, the added risk of cybersecurity threats may dissuade potential purchases. Is it possible that individuals and enterprises believe that IT systems increase risks, and thus are not participating in global trade?

Costs of data protectionism. Cloud computing benefits from the economies of scale. National policies mandating geographic and legal restrictions may well increase costs by reducing efficiency and increasing support costs. Yet little is publicly known about these expenses, or how they would affect international competition. How do checks on cross-border data flows change the economics of cloud computing, and can they be mitigated with technical solutions?

Cybersecurity Ghettos. If developed countries face cybersecurity risks through their dependency on IT, they at least have more resources to deal with it. As developing countries grow more dependent on IT, they may not invest in securing it (any more than some of the wealthier countries are, of course). If cyber criminals shift their targeting to poorer, less secured countries, this could create a ghetto of sorts. Should we expect a rise in attacks on the developing world, and will technical interdependence put others at risk?

Substitutions around trade barriers. If domestic regulations do create trade barriers and distort the market, how will the affected consumers react? Different products have different

price elasticities, and different complementary technologies. How could substitutions alter the IT landscape, particularly for concentrated markets?

Economic Impact of the Common Criteria. Before the Common Criteria (CC) for Information Technology Security Evaluation was standardized in 1998, vendors had to evaluate the same product for multiple countries. While the IT market may have evolved too much to compare pre-CC markets with contemporary markets, some quantitative analysis should be possible. How has the Common Criteria changed the global IT market?

RECOMMENDATIONS

While this is a relatively new policy problem that deserves further study, there are some basic recommendations to avert the larger harms. Fortunately, we are still in the early days of addressing these threats, and few countries have fully committed to a single approach. Indeed, the slow pace of government policy that many security experts decry may have a silver lining if these moderating steps below are taken. They fit into four areas of prescription: enhancing security capacity, harmonizing standards, avoiding obstacles to the flow of data and promoting trade as a means to achieving security. These four directions are complementary, and must be pursued simultaneously.

Enhancing cybersecurity capacity involves understanding the risks at a technical level and an international one. On the technical level, leaders should *demonstrate actual security benefits from policy initiatives*. While the challenges of "provable" security and metrics will not be solved anytime soon, it should be the inspiration and the starting point.

In a world connected by digital networks and trade networks, it is not enough to defend yourself. Beyond their own borders, developed countries should *promote global cybersecurity capacity building*. Cybersecurity is a global problem. If developing countries do not have the capacity to defend their networks, it puts the world's systems at risks for cyber attack, and may harm global trade through reduced demand or the promotion of domestic standards.

Countries should instead *emphasize international or harmonized security standards*. Shared standards enable security without erecting barriers to trade. At the same time, we should not expect a single, global standard for all IT. All security management processes reflect a trade-off between the guarantees they afford and the costs imposed. *Policies and priorities should reflect these trade-offs*, with a process that can accommodate an evolving technical and security landscape. Governments must also learn to *balance specific security needs with the benefits of a generalized process*. Some sectors have specific security requirements, which can complicate global trade if the bureaucracies fail to coordinate. On the other hand, a generalized security standard allows more efficient access to global markets, but can over- or under-protect the critical infrastructure in question. Finally, *standards processes should be as open as possible*, and participants should work to minimize political conflicts in the standards process.

National politics should also play a minimal role in the new era of cloud computing. *Data protectionism should be strongly discouraged*, particularly any mandates about geographic location of data centers. When governments do intervene with the flow of data, *states must agree to fair and equal transparency rules*[41] for all data users, particularly foreign citizens.

Finally, trade and diplomacy need an equal seat at the table in cybersecurity discussions. Trading partners and stakeholders must work together to *discourage national security exceptions* that could threaten the stability of global trade. The WTO has more appropriate venues[42] for this kind of discussion without the specter of mutually assured destruction. In general, *diplomatic and trade voices can serve as a check against the temptations to abuse the cyber domain*.[43] While security is a priority, other voices can help put the risks of being overly aggressive or overly cautious in a context of other national interests.

CONCLUSIONS

This paper addresses the intersection of two of the largest dynamics shaping our world today: the connectivity that arises from global trade networks and global data networks, and the risks introduced by that connectivity. Just as countries around the world have grown more dependent on information systems for their stability and quality of life, they have also grown dependent on the trade that supports IT access and innovation. Threats to IT systems have spurred governments to think about regulatory solutions, but care must be taken not to disrupt the parallel system of trade that undergirds the IT ecosystem.

At the same time, there will still be debate and study about the respective merits of government involvement in regulating cybersecurity and the social costs and benefits of free trade. I argue that these discussions should inform each other. With respect to cybersecurity regulation, we are still in the early days of understanding what the government role should be, and what regulatory tools are available. Policymakers and stakeholders should take security risks seriously, but be careful that their attempts to strengthen one network do not irreparably harm the other.

41 The transparency rules laid out in this report are an excellent start: Joshua Meltzer, "The Internet, Cross-border Data Flows and International Trade" Brookings Issues in Technology Innovation. Issue 22. (2013). http://www.brookings.edu/research/papers/2013/02/25-internet-data-flows-international-trade-meltzer

42 Ahrens, Nathaniel. "National Security and China's information security standards" CSIS Hills Program on Governance. (2012). https://csis.org/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf

43 Friedman, Allan. "Why Wasn't the NSA Prepared?" *The Atlantic* (August 2, 2013). http://www.theatlantic.com/national/archive/2013/08/why-wasnt-the-nsa-prepared/278310/

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance.aspx

Editor
Christine Jacobs
Beth Stone

Production & Layout
Beth Stone

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU