Cyber Threats and Their Effect on the International Political Economy:

Non-Tariff Barriers to Trade and the Digital Revolution

Sean M. Sarich
The Pennsylvania State University
Sjs6728@psu.edu
November 10, 2019

Author Note:

This paper has been prepared for PLSC 412: International Political Economy, Sect 001, Fall 2019, instructed by Professor Tamar London, Ph.D.

Introduction

When one thinks of cyber threats, the mind often drifts to soundbites of the latest breach of user metadata or perhaps a Tweet about the sudden encryption of a company's system only to find out that a hacker is holding the data ransom for a sum of money. Such stories seem to occur almost daily across the globe as interconnected digital systems expand into our social spheres, automating most common tasks. These conveniences range from simple items, like regulating the heating and cooling in our homes to interfacing with more critical information like banking, medical records, and even the very power that makes it all possible. While most of the stories surrounding an interruption of these conveniences tends to focus on the impact either monetarily or emotionally on the user, there is a far less dense array of reporting and academic focus on how these threats go on to impact more expansive aspects like regional populations, governments, international security, and—as the subject of this research endeavor—the factors that impact the international political economy (IPE). In light of the research scarcity that surrounds the confluence of cybersecurity and the IPE, the focus of this analysis is based on the following line of questioning: how do cyberattacks and cyber threats impact the broader global economy?

The answer to this question is far more complicated than merely noting the monetary losses that are a common byproduct of interrupted services after a successful cyberattack. Since the reach of interconnected information technology has augmented human behavior to the point of near-dependence, cyberspace has become an entirely new domain of conflict and consideration within the international system. As far as the IPE is concerned, cybersecurity has led to new insecurities and policies that have created new relational obstacles that have a yet-to-be-fully-determined effect on international trade discourse. Classically, similar constructive obstacles have been called *non-tariff barriers* to trade (NTBs) and have taken the form of the

arbitrary determination of goods as dangerous, antithetical to good business practice, or in threatening aspects of the public health. With the abstract nature of networked infrastructure connecting so many services, critical or otherwise, the tactic of leveraging the anonymity of cyberspace to carry out certain information operations by the world's largest powers leaves open the opportunity for information security to twist classic NTBs into maneuvers that are part of a larger strategy. To test the merit of cyber threats as NTBs, then, the case study analyses of US trade relations with Russia, China, and the European Union has been commissioned and favors the conclusion that cyber threats create non-tariff barriers to trade through modifications to national security policy, foreign direct investment and intellectual property policy, and by way of the technical requirements established by the domestic market demands within each country.

Literature Review

Consequences of Cyber Security Considerations on International Trade Policy

Given the nascence of cybersecurity as a broad concern in contemporary popular culture, the effects of information technology on international trade are only recently garnering attention. While the research contained herein surveys the relationship between cyberattacks and international trade barriers, the genesis for this topical matter can trace its core back to the work of Allan A. Friedman of the Brookings Institute and his 2013 research paper *Cybersecurity and Trade: National Policies, Global and Local Consequences.* Within, Friedman theorizes that barriers to trade with the most economic impact will likely revolve around states' national security policies, foreign direct investment and intellectual property policies, and technical requirements. For the sake of both current and future research, it is important to understand the implications of these effectors and how they might be leveraged in future trade disputes and in confluence with strategic-trade theory which typically explains both tariff barriers and non-tariff

barriers in tech-related sectors and as a part of broader political agendas (Rugman and Verbeke, 1990).

In the case of national security policy, Friedman (2013) cites the use of trade restrictions in durable security frameworks as a strategic measure, not unlike the employment of economic sanctions. The main difference between the use of economic sanctions and citing preexisting national security frameworks becomes the show of force in the former and a more passive-aggressive and nebulous policy in the latter. As an example, instead of making more obvious protectionist policies that might indicate a bias of aggression, policymakers can point to something like the Cybersecurity Framework (CSF) in the US whereby restrictions on the procurement of IT products can be employed "to promote the protection of critical infrastructure" (NIST 2013). Friedman goes on to cite the escalation environment that then becomes harmful to free trade as cyberattacks begin to mar the credibility of international actors such as was shown in the now infamous US-Israeli Stuxnet attack against Iranian nuclear facilities in the late 2000s (Zetter 2015).

Somewhat related to the national security argument is the concern over foreign direct investment (FDI) and intellectual property (IP) policies. The conventions of strategic-trade theory become more apparent here as FDI can bring manufacturing to a regional center that favors a particular state. Given the scarce security and governance in some of these regional centers, the rise in IP theft is multiplying damages to credibility as 'knock off' producers pop up and minimize the need for free trade. In both cases, the blinding pace at which IT is both developed and brought to market means that there is a constant battle over which state hosts this innovation and how developments in the IT sector might bolster power positions within the international trade system. Of course, the threat of IP theft is of major concern in countries like

China that hope to out develop and undercut other major actors like the US in these design and innovation segments in an effort to garner more economic leverage within the international system (USTR.gov, 2018). This certainly gives rise to protectionist groups that are affected by DFI and IP theft anxieties that often look to national security policy and international law bodies for protection.

While both national security and DFI/IP policies tend to manifest NTBs from both a tactical perspective and from the more earnest perspective of protecting constituents, concerns over technical standards serve as the most prevalent NTB since they are the most abstract. As a byproduct of fast movement, constant innovations cycles, and security compliance as-driven by other factors such as cybercrime and general user privacy, the technification of all market sectors has given rise to an ever-evolving list of needs from the international economy. Since these needs can range from obvious, if there are limited producers of difficult to source products, to nebulous, as we see in the protection of the broadly termed genre of *critical infrastructure*; standards themselves can be a trade barrier if only as dictates of price and trade flow (Friedman 2013, 13).

Codifying the Terms of Trade Under the Threat of Information Security Concerns

Perhaps in spiritual if not direct succession of Friedman, the work of Huang, Madnick, and Johnson in *Interactions Between Cybersecurity and International Trade: A Systematic Framework* (2018) serves to offer some of the explanative mechanisms that cause the international political economy to react to the concerns over cybersecurity. Moreover, the core of Huang, Madnick, and Johnson's argument tends to hinge on the involvement of multinational corporations (MNCs) as the panacea to the many issues that plague the discourse regarding cybersecurity and its effect on international trade. They offer that MNCs, through cooperation

and readiness, can negate several of the significant NTBs listed by Friedman—that "cybersecurity concern pressure can even be used to improve the global supply chain and create a competitive advantage" (Huang, Madnick, and Johnson 2018, 1).

This perspective is gleaned from the complexity of the information security premise: the analysis of an unimaginable amount of code and content across the many disparate systems that comprise the whole of the Internet. Since MNCs are the most proximal to their markets by default, using mitigating techniques to preserve the market, then compete are thought to be the nurturing fabric that can absorb some of the focus away from the government trade regulations that are often rooted in national security policy. Coincidentally, the authors cite the involvement of MNCs in global supply chain cyber risk management and policy implementation as a way to "avoid a 'cyber cold war' in the global digital economy" (Huang, Madnick, and Johnson 2018, 3) as demonstrated by the US-China Trade War of 2018.

Cyberattacks: Criminal Enterprise, Trade Tactic, or Act of War?

In Andy Greenberg's *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Greenberg investigates the complications that present themselves to the international community when state-attributed cyberattacks cause widespread devastation to critical infrastructure and the global supply chain. Greenberg's account seamlessly blends with the theoretical suppositions in the work of both Friedman *and* Huang, Madnick, and Johnson by demonstrating that the favor of national security policy in informing government-led trade policy. Moreover, Greenberg shows that the favor towards national security is not a baseless premise that hangs on ceaseless *what-if* trepidations and/or *bad blood* politics. In this particular case, Russian attribution in the NotPetya attack that caused billions of dollars of damage internationally changed the way that countries have interacted with Russia. For the US's

part, the attack was looked at as part of an ongoing cyber struggle that has witnessed escalation for both sides since Russia's alleged involvement in the 2016 presidential election in the US (Sanger and PerlRoth 2019).

As part of Greenberg's broader theories, blatant attacks like NotPetya are shown to foster NTBs on the basis of distrust, harkening back to the importance of credibility when it comes to international trade. In the Russian implication of NotPetya, there is a new dialog over the use conditions of cyber implements and how they might be considered as acts of war. Alas, the amorphic nature of *cyberspace* as a term for the logical environment that comprises interconnected IT systems is one that seems to suffer from an equally broad interpretation of cyber law or cyber policy language. As an example, it could be supposed that IP theft may just as well be considered larceny by someone like the US versus a gain in competitive advantage by someone like China. Likewise, the ambiguity and anonymity afforded by cyber operations can be employed with minimized risk by actors such as the Russians who may be seeking to challenge the perceived hegemonic advantage appended to the United States. In either case, restrictions to free trade are easily concretized over by generalized national security policies, just as Friedman suggested in his 2013 piece. By virtue of the MNCs at the core of Greenberg's narrative, however; the logic of Huang, Madnick, and Johnson gains a fair amount of support in that market protection and standardization can act as a buffer between nefarious cyber actors and NTBs that might result from more staunch national security policies in the wake of a successful attack.

Case Study Analysis

Method

The following case study analyses feature a survey of reactive politics that function to dissect the aforementioned literary entries in an effort to scrutinize their fledgling frameworks against the IPE of the present day. Much of the language that either supports or denies the effects of cybersecurity on national security policy, foreign direct investment and intellectual property policy, and by way of the technical requirements established by the domestic market demands within each country are found within policy addendums and through the rhetoric of key leadership. The goal of this analysis is to address these public-facing entries and relate them to their implied validation of cyber NTBs.

Results

Case Study #1: The United States and Russia: Cyberwar is the New Cold War

In the case of the US and Russia, the nefarious bent of Russian state-sponsored cyber groups transcends the social engineering campaigns aimed at steering Western hegemony as exemplified in the 2016 presidential elections. The detailed account of Russia's attempts to access areas of US critical infrastructure, to include power and utility companies, in Greenberg's *Sandworm* are issues that have not been overlooked by the US defense sector. Moreover, the sheer magnitude of the days long Notpetya attack that crippled the Maersk shipping company and, in the words of Greenberg, "the world's most complex and interconnected distributed machines, underpinning the circulatory system of the global economy itself" (2019, 192), would signal to the US and the world that Russia possessed devastating electronic weapons with unprecedented global reach. In turn, this has gone on to affect the posturing of the US in its dealings with Russia, only deepening the trust division between either country—something proven by the United States' recent defense bill that has authorized

increased cyber research, exploitation, and deterrence against Russia that was passed in the late summer of 2018 (Sanger and Perlroth 2019).

Standing with the open leverage of escalations rhetoric in the case of the uptick in US operations against Russia, the language surrounding US trade policy and sanctions against Russia contains over 70 references to the word "cyber" in a study conducted by the US Congressional Research Service in January of 2019. What's more, the language of the report is rather direct in its allusion that in concert with viewing sanctions as "central element of US policy to counter Russian malign behavior" (Welt et al. 2019), election interference and cyberattacks are key line items that are meant to challenge Russia's overt use of cyber capabilities in information operations against the United States. In many ways, these modern sanctions seem to echo the soft-belligerence conveyed by similar Cold War-era trade language in policy such as the Jackson-Vanik amendment of 1974 that used human rights concerns to adjust US-USSR trade provisions. Basically stated, the US and Russia seem to demonstrate little in the way of divergence from this classic Cold War competition that often utilized economic policy as a proxy for physical conflict.

Given the resurgence in Cold War-style policy motives in that case of the US and Russian, the increasing conditional aspects for domestic market procurement are shown to extend trade complications beyond formal sanctions as previously mentioned by Friedman in 2013. Though more detail over the restriction of imports due to certain industry compliance measures will be mentioned further when discussing Chinese IP gathering, it should be noted that the parallel in citing compliance criteria to a figurative *witch hunt* allows for a better understanding of how ad hoc action can be taken on the import and export of goods simply by citing trade rules that can be broadly interpreted. In this case, Russian high technology goods are

often restricted from being used in US information systems for fear of state meddling that may allow for hackers to gain backdoor access to American Critical Infrastructure (NIST 2013). Simply stated, the rise in cyber-related NTBs between Russia and the US are the product of constant antagonism coupled with 'catch-all' policies that can be used without either country taking an official stance towards the other.

Case Study #2: The United States and China: The Effects of Intellectual Property Hoarding

As it pertains to China and its widely reported habit of hoarding US intellectual property, the US has leveraged the issue heavily in the US-China Trade War of 2018. Moreover, the fear of infiltration has spawned increased distrust between the two nations in terms of incorporating imported technology into critical systems. On the US side, this security endeavor is codified as the CSF under NIST, while on the Chinese side, it is referred to as Article 37 of the Cybersecurity Law (Keman, Madnick, and Johnson). The lever of these laws is illustrative of how policy restrictions encourage protectionism—something cited in appeals to the US Trade Representative by several large corporate entities.

This is a textbook example of strategic-trade theory and can be expected to mirror high technology and agricultural protectionism. Since theft, shifts in sourcing, or the relocation of industrial standards bodies are widely known to hurt commerce, the fear driven restriction and 'tit for tat' exchange between both countries can cause hesitations in the international market. Additionally, the incentives to produce products domestically to overcome security concerns will lead to subsidies for domestic enterprise while reducing that the incentives for foreign direct investment. Once again, the NIST and CSF provisions for information technology in both China and the US curate a 'catch all' framework for this protectionist mechanism that parallels the US-

Russia case study in that either country can enforce NTBs without expressing an official position such as they would by inmposing tariffs or sanctions.

Case Study #3: The United States and the European Union: Prototyping a Framework

US-EU cyber policy has been, for the most part, mutually supported. This has been demonstrated in the US-EU's "Safe Harbor" policy that has allowed information sharing for the sake of transnational criminal investigations. Moreover, the cooperation between the EU and the US can be found in the confluence of interest in combining effort in sanctioning Russia. This is outlined in the US and EU Sanctions Cooperation and was the result of the rally around Russia's move to take Crimea from Ukraine—a Russian operation that used similar TTPs involving cyber and electronic warfare activities before invading Estonia.

Despite an alignment on many issues relating to information technology and security, the US and the EU must still observe compliance regulations set forth by each country. Though these compliance standards are laxer when compared to the US or China, they can still become NTBs when considering the abstract nature of compliance and trade language. In this sense, NTBs can be thought of as somewhat less as an extension of national security policy and more as a means for the EU to gain a competitive advantage as explained under strategic-trade theory. This juggle between domestic profitability and international trade is fairly standard for most verticals, however in knowing that the EU countries and the US benefit from decentralizing defense initiatives there will always be a drive to minimize risk from the security perspective just as there is from the commerce perspective.

Discussion/Conclusion

The use of information systems as a tool of power and policy have ushered in a new era whereby all facets of human relations can be affected with little regard for time and space. As far

as the IPE is concerned, NTBs as a result of cyberattacks or the threat of cyberattacks falls perfectly in line with previous frameworks and has been furthered by the continuation of IP theft by China and the devastating NotPetya attack that stemmed from Russia. Moreover, the prevail of strategic-trade theory in explaining cyberspace in the economic context indicates that the construct of cybersecurity is then a mixture between the high technology market and international security. Additionally, it would seem that there is further support for these security-driven mechanisms can be found within existing international relations theories. In this case, democratic peace theory may explain the confluence of interested between the democratic commonality of the US and the EU compared to the hostility that exists between US democracy and the autocracies of Russia and China. It could be argued, then, that despite the barriers for trade mentioned above, complications in the IPE caused by cybersecurity considerations could be an extension of a much larger contrivance of conflict.

As global supply chain and critical infrastructure automation continue to grow, then so too will cyber-related NTBs. With more systems becoming attached to IT infrastructure, there will need to be continuous monitoring of how national security policies, foreign direct investment and intellectual property policies, and technical compliance policies will evolve to deal with a broader digital attack surface. Also, as can be surmised from the case study material regarding the NotPetya attack, the possibility of a much more extensive and damaging attack is entirely possible. As it were, it will be necessary for those in risk management and economics research to factor in potential future damages to adequately prepare an appropriate incident response plan.

To conclude, Non-tariff barriers to trade are unavoidable side effects of the political discourse in that the global supply chain has become the means by which most of the world's

population sustains itself. Given this precedent, the automation of the global supply chain has created a new paradigm whereby NTBs can be hidden within somewhat amorphous defense policies, suspicions of state-sponsored espionage, and compliance measures that must be heeded in order to protect critical infrastructure. Essentially, the convenient leverage of cyber-related NTBs has been shown in the above case studies only further to complicate the IPE and the future of trade negotiations.

References:

Friedman, Allan A. 2013. "Cybersecurity and Trade: National Policies, Global and Local Consequences." *Brookings Institute Center for Technology Innovation*. https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsCybersecurityNEW.pdf (September 29, 2019).

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday.

Huang, Keman, Stuart E. Madnick, and Simon Johnson. 2018. "Interactions Between Cybersecurity and International Trade: A Systematic Framework." *MIT Libraries SSRN Electronic Journal*. doi: 10.2139/ssrn.3370562.

Myre, Greg. 2017. "U.S. Sanctions Against Russia Never Go Away - They Just Evolve." *NPR*. https://www.npr.org/2017/07/21/538086476/u-s-sanctions-against-russia-never-go-away-they-just-evolve (November 11, 2019).

NIST. 2013. "Discussion Draft of the Preliminary Cybersecurity Framework." *NIST.gov*. https://www.nist.gov/document-4543 (October 13, 2019).

Office of the United States Trade Representative. 2018. "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974." *Office of the United States Trade Representative, Executive Office Of The President*. https://ustr.gov/sites/default/files/Section 301 FINAL.PDF (October 13, 2019).

Rugman, Alan M., and Alain Verbeke. 1990. “Strategic Trade Policy is Not Good Strategy.” *Hitotsubashi Journal of Commerce and Management* 25(1): 75–97. http://www.jstor.org/stable/43294924 (October 13, 2019).

Sanger, David E., and Nicole Perlroth. 2019. “U.S. Escalates Online Attacks on Russia's Power Grid.” *The New York Times*. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (October 13, 2019).

Turak, Natasha. 2018. “US Will Impose Costs on Russia for Cyber 'Acts of Aggression,' White House Cybersecurity Czar Says.” *CNBC*. https://www.cnbc.com/2018/02/16/us-will-impose-costs-on-russia-for-cyber-aggression-says-cybersecurity-czar.html (October 13, 2019).

Welt, Cory, Kristin Archick, Rebecca M. Nelson, and Dianne E. Rennack. 2019. “U.S. Sanctions on Russia.” *Congressional Research Service*. https://fas.org/sgp/crs/row/R45415.pdf (November 10, 2019).

Zetter, Kim. 2015. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown Archetype.