The Next Global Financial Crisis Could Be Caused by Efforts to Prevent the Cyberattack

Keman Huang[1,2(✉)] and Stuart Madnick[2]

[1] Renmin University of China, Beijing 100086, China
keman@ruc.edu.cn
[2] Cybersecurity at MIT Sloan, MIT, Cambridge, MA 02142, USA
smadnick@mit.edu

Abstract. In the era of Web-based services and Internet-of-Things (IoT), almost every product and service is Internet-connected. Providers want their products and services to capture data, in part to improve performance and consumer satisfaction, but these might also be tools for spying and other malicious activities. Hence cybersecurity has increasingly been invoked from the perspective of "national security," directly impacting international trade and investment policy. The press has largely focused on trade issues between the USA and China, especially regarding Huawei. However, the scope of such cybersecurity impacts goes far beyond these two countries. As part of our research investigation, we identified and analyzed 33 cases, which involved 19 countries. So this is a truly global phenomenon that needs to be addressed. This paper presents a taxonomy developed to understand the different circumstances, actions, and outcomes.

Keywords: Cybersecurity · International trade · Trade restrictions · Financial crisis · Cyberattack

1 Introduction and Motivation

There have been headlines like "A cyberattack could trigger the next financial crisis" [1] and "How a Cyberattack Could Cause the Next Financial Crisis." [2] These should be of concern to all of us and be important incentives to do something. But what should be done? As we explain in this paper, actions taken to prevent such a cyberattack may, in fact, be the actual cause of a major financial crisis – even a global international trade crisis.

Issues of international trade policy have gained increased attention. Of course, restrictions on international trade regarding technology have long existed – on imports and exports, as well as on direct foreign investment. But cybersecurity has not been a key issue for trade policy – until now.

In the era of Web-based services and Internet-of-Things (IoT), almost every product and service is Internet-connected. Manufacturers want their products and services to capture data, in part to improve performance and consumer satisfaction, but these might

A. Garimella et al. (Eds.): WeB 2020, LNBIP 418, pp. 3–11, 2021.
https://doi.org/10.1007/978-3-030-79454-5_1

also be tools for spying and other malicious activities. Hence cybersecurity has increasingly been invoked from the perspective of "national security," with a direct impact on international trade and investment policy [3–6].

Furthermore, data is considered a critical asset that supports digital service industries with increasing concern about data sovereignty [7]. As a result, it is not just products that would be impacted, but also services, such as international banking and payment systems [8]. We have recently seen effects to restrict or ban web services such as TikTok and WeChat [19].

From a defensive perspective, since it is impossible to thoroughly examine the millions of lines of software or firmware in these products, what should countries do to prevent cyber intrusions when these products can introduce cyber attack vectors? One approach that has been often suggested and increasingly implemented is excluding any potentially dangerous products or services coming from questionable countries. But this raises important policy issues, such as (1) what is a dangerous product or service and (2) what a questionable country is? Assuming such restrictions quickly become worldwide policies with retaliations, what might be the ultimate impact on international trade and the economy? Possibly a major financial crisis.

As an effort to explore ways to maintain an open and cyber secure international trade system and avoid the above dilemma, this paper aims to understand the current landscape of how countries and companies manage cybersecurity issues within the digital trade system. Based on the 33 cases we identified, our preliminary results demonstrate that such cybersecurity is an increasing global governance issue. The diverse actions and outcomes highlight the essential requirement to construct a global governance framework to avoid a recurrence of the "Smoot-Hawley Tariff" disaster within the digital age.

2 Literature Review: Cybersecurity Within Digital Trade

Cross-border data flows play a critical role in digital trade. Most studies about the linkage between digital trade and restrictive policies focus on data restriction policies, such as data localization or privacy regulations [20]. For example, increasingly regarding Artificial Intelligence (Al), trade policies related to privacy, data localization, privileged access to government data, industrial regulation related to standards and source code, can have a negative impact on international trade [21]. However, the digital trade policies due to cybersecurity concern are much broader than just the data restriction policies [22] and include policies related to tariffs on digital goods, filtering and blocking, Intellectual Property Rights (IPR) infringement, national standards, and burdensome conformity assessment and regulations to limit disinformation, etc.

On the other hand, the reterritorialization of cyberspace as a national cyber territory has become a reality [7], and many nations have expanded or are expanding their authority into cyberspace. Many studies discuss cybersecurity within digital trade from the international relation context and explore how cybersecurity changes international governance [23, 24]. We are also witnessing cybersecurity concerns regarding digital trade reshaping the international business environment, and international corporations need to understand the associated risks [9]. However, the interactions and outcomes are highly diverse due to the dynamics among countries (both host and home countries) and corporations (both domestic and international enterprises).

This study aims to unfold the phenomenon around cybersecurity governance within digital trade and create an overview framework to explore the different implementations of policies and the dynamics among countries and corporations.

3 Methodology

As part of our research investigation [9], we used "cybersecurity" and "international trade/digital trade" as the keywords to search the news. Then we went through the relevant news and only considered those cases that involved at least two countries. For each case, we further collected publicly reported interactions among those countries and companies to grasp the dynamics within each case. For example, for the Huawei case in the USA, we can trace back to 2008. Digesting these cases enables us to develop a preliminary framework, focusing on the different actions that countries and corporations took. We further hosted workshop discussions with senior executives, managers, and researchers from Fortune 500 companies, and cybersecurity solution providers who are industrial members of our consortium, Cybersecurity at MIT Sloan (CAMS), to discuss these cases and identify additional cases. We repeat this process to add cases and verify the developed framework.

Through this process, we identified at least 33 cases, which involved 19 countries, and developed the framework we reported in the following sections. Note that in this study, we don't intend to develop a comprehensive case library but focus on the coverage of the diverse countries, products/services, actions, and outcomes.

4 A Glance on the Increasing Scope of Impact

The press has largely focused on trade issues between the USA and China, especially regarding Huawei and now TikTok and WeChat. But the scope of such cybersecurity impacts goes far beyond these two countries. As shown in Fig. 1, the 33 cases we identified have involved 19 countries.

Fig. 1. Countries that instituted international trade restrictions due to cybersecurity concerns

When these cases are studied, a complex web of impacts quickly becomes clear, as shown in Fig. 2. The point is that, even at this rather early stage, this is already a worldwide phenomenon and growing. In Fig. 2, the direction indicates the source nation to impacted nations (note: many go in both directions), and the number indicates the number of occurrences in our collection of 33 cases.

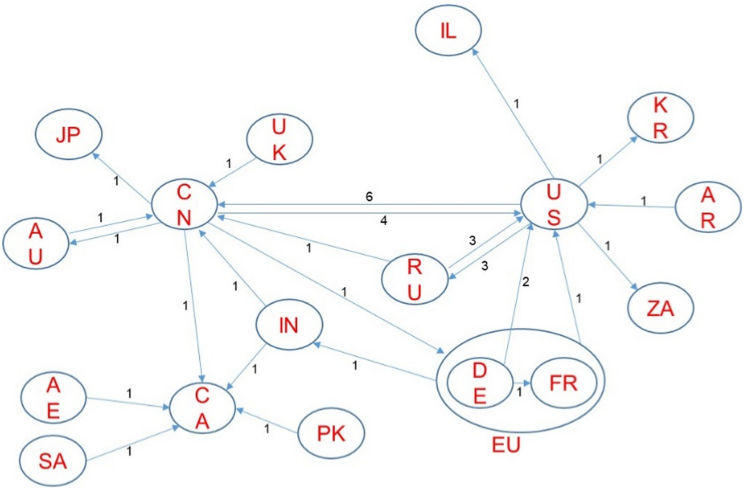

Fig. 2. Network diagram of ccountries with international trade restrictions due to cybersecurity concerns

As just one example regarding the voice-activated 'My Friend, Cayla' doll, made in the U.S., there was a concern that potentially it could spy on children or anyone in the room, collecting personal data, so "On 17 February 2017, Germany banned both the sale and ownership … alleging that it contains a concealed surveillance device' that violates federal privacy regulations." [10] There are many other such cases. Increasing prohibitions on the import or export of products and services could certainly have an impact on international trade and world economies. But, there can also be even more direct impacts. Currently, there are over one quadrillion dollars, that is 1000 trillion, a year of cross-border monetary payments. Consider this real headline, "Amazon sellers get caught in US-China trade spat as money transfer service abruptly closes." [11] What caused the problem? The answer was that "U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns." [12].

5 Framework for Studying Cybersecurity Impact on International Trade

We have developed a framework, shown in Fig. 3, to systematically organize the details of each of the cases identified, especially the timeline, related actors, actions, and impacts for each case. This framework focuses on demonstrating the dynamics of the cybersecurity impact on international trade and addresses not only compliance issues, but also the business and geopolitical issues.

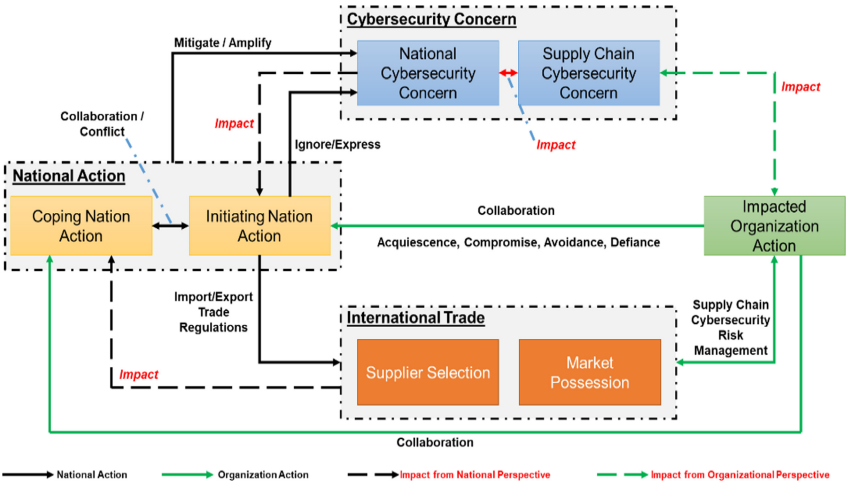

Fig. 3. Framework for the impact on cybersecurity concern on international trade

Scope of National Cyber Security Concerns. The definition of national cyber security is often intentionally vague to achieve some operating space [13], but there is no doubt that national cyber security is a multi-dimensional concept, and all the different perspectives must be considered, including military security, political security, economic security, and culture security. Most organizations, not only businesses but also governments, are becoming increasingly reliant on global supply chains, including both digital and physical supply chains. The most famous example using the supply chain vulnerability was the Stuxnet attack on the Iran nuclear enrichment facility. It was allegedly accomplished by planting malware in the industrial control system, which was then shipped to Iran, resulting in the destruction of many centrifuges [14]. Note that national cybersecurity and supply chain cybersecurity are not isolated. For example, the U.S. Department of Defense (DoD) "buys products from international commercial and mixed defense and non-defense companies that service many customers, both within and outside of defense markets" [15].

Hence, the cybersecurity of the supply chain for critical infrastructures will raise concerns about the nation's cybersecurity. On the other hand, the concerns of national cybersecurity impact the perception about the risks from supply chains and further impact the business' concerns on the supply chain cybersecurity.

Different Actions and Dynamic Outcomes Possible. There are many different circumstances, leading to different actions and outcomes. Using the framework above, the actors, actions, and impacts for each of the 33 cases studied are studied and reported in [16]. Figure 4 gives a high-level summary, the 33 cases are across the horizontal, and the differing circumstances, actions, and outcomes are along the vertical. A checkmark with a yellow marker is shown whenever the circumstances, actions, and outcomes apply. The critical thing to note is that even with this relatively small sample of cases, there is a wide variety of cases and actions. The reader is referred to [16] for the details.

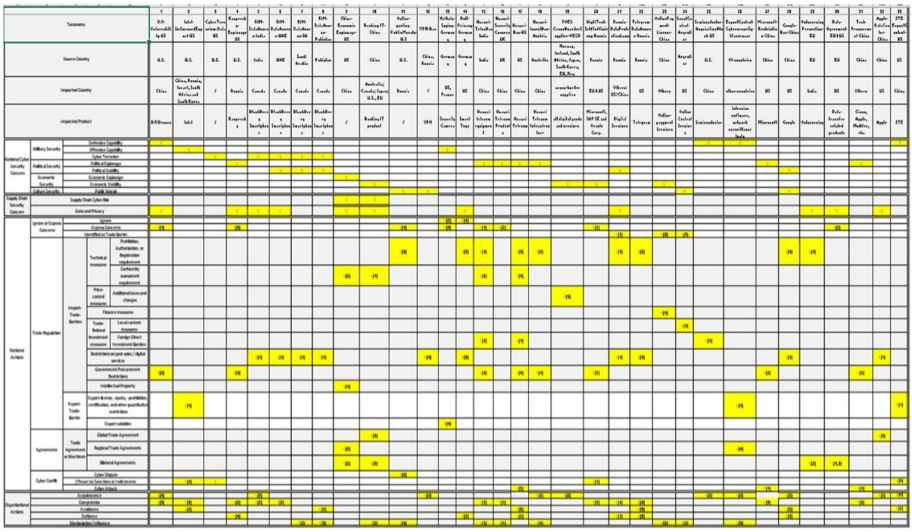

Fig. 4. Matrix listing the cases studied and their differing circumstances, actions, outcomes

To illustrate some of the diversity, we will briefly discuss just two cases with different outcomes. These are cases involving Huawei in the U.S. and U.K. as examples of different actions and outcomes.

In 2011, worried about potential spying, the U.S. government blocked a bid from Huawei to help build a new national wireless network for first responders such as police, firefighters, and ambulances. In 2012, the U.S. further released a report urging U.S. telecommunication companies not to do business with Huawei Technologies Co Ltd and ZTE Corp because it said potential Chinese state influence on the companies posed a threat to U.S. security. In 2013, Washington ordered several major government departments, including NASA and the Justice and Commerce Departments, to seek approval from federal law enforcement officials before purchasing I.T. equipment from all Chinese vendors, requiring the agencies to make a formal assessment of "cyber-espionage or sabotage" risk in consultation with law enforcement authorities when considering buying information technology systems. Finally, in 2014, Huawei decided to exit the U.S. market largely.

On the other hand, in 2010, Huawei opened its Cyber Security Evaluation Centre in the U.K. "The new Cyber Security Evaluation Centre is a key part of Huawei's end-to-end global security assurance system. This center is like a glasshouse – transparent, readily accessible, and open to regulators and our customers." [17] In 2013, when the parliamentary intelligence and security committee (ISC) raised concerns that Huawei's equipment could be used by Beijing to spy on the U.K., and called for an urgent inquiry, the U.K. National Security Adviser published the executive summary to the ISC on a review of Huawei's Cyber Security Evaluation Centre (HCSEC), concluding that "The review judged that the HCSEC was operating effectively and achieving its objectives". In early 2014, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, was further established on the recommendation of the U.K. National Security Adviser to

oversee and ensure the independence, competence, and overall effectiveness of HCSEC. Every year it releases a report about any risks to U.K. national security from Huawei's involvement in the U.K.'s critical networks and makes sure that these risks have been sufficiently mitigated.

Hence, though the U.S. continues to lock Huawei out from its 5G market, on 28 January 2020, it was reported that "U.K. government approves Huawei 5G deal." [18]. Note that due to the dynamic political environment between the USA, China, and the U.K., on July 14, 2020, the U.K.'s decision is changed again, requiring telecom operators not to buy any new equipment from Huawei after the end of 2020 and remove Huawei equipment by 2027.

6 Example from the Past: Smoot-Hawley Tariff

Let us now look to the past to see how there could be a major breakdown of international trade, and how that could create a global financial crisis. In the aftermath of the stock market crash of October 1929 and the following impacts on the economy, the U.S. Congress enacted the United States Tariff Act of 1930, commonly referred to as the Smoot-Hawley Tariff. It increased tariffs on foreign imports to the U.S. by about 20% on top of already high import duties on foreign agricultural products and manufactured goods. But what were the consequences? At least 25 countries responded by increasing their own tariffs on American goods. As a result, global trade plummeted, in the USA there was a reduction of exports and imports by 67%, contributing to the ill effects on the world economy. In essence, it made the Great Depression much greater!

This mishap was finally reversed, starting with the Reciprocal Trade Agreements Act of 1934. But, the increasing use of international trade barriers and restrictions discussed earlier, followed by retaliations, could produce a similar chain of events. It would be good not to see history repeated.

7 Conclusion

With the increasing development of and dependence on the digital economy, cyberspace plays a critical role in international trade. We have found many ways that cybersecurity concerns can impact international trade. As part of our research investigation, we identified and analyzed 33 cases, which involved 19 countries. So this is truly a global phenomenon that needs to be addressed.

Due to the lack of consensus on cyberspace behavior norms and the vague definitions of national cyber security, we can expect even more cyber conflicts and their negative impact on international trade.

However, instead of each nation proposing its own set of norms that will inevitably be at odds with one other, finding common ground and working together to construct cyber norms is an important task.

Also, instead of only considering cybersecurity a regulation issue and trying to comply with the emerging regulations, companies should become actively involved in the regulation processes, not only during the comment periods but also during the regulation draft process. With a cool mind and careful academic study, effective norms can be developed, and the worse case scenarios can be avoided.

Acknowledgment. This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

References

1. Pisani, B.: A cyberattack could trigger the next financial crisis, new report says. CNBC (2018). https://www.cnbc.com/2018/09/13/a-cyberattack-could-trigger-the-next-financial-crisis.html
2. Mee, P., Schuermann, T.: How a cyber attack could cause the next financial crisis. Harvard Business Review (2018). https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis
3. Friedman, A.A.: Cybersecurity and Trade: National Policies, Global and Local Consequences. Brookings Institution Center for Technology Innovation (September), pp. 1–18 (2013)
4. Kshetri, N.: Cybersecurity-Related Barriers to International Trade and Investment. The Quest to Cyber Superiority (2016). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809819
5. Mata, D.C.: Cybersecurity dimensions of national security. J. Law Admin. Sci., 132–142 (2015)
6. Farrell, H., Newman, A.L.: Choke Points. Harvard Business Review, February 2020
7. Lambach, D.: The Territorialization of Cyberspace. Int. Stud. Rev. **22**, 1–25 (2019). https://doi.org/10.1093/isr/viz022
8. Huang, K., Madnick, S.E.: Cyber securing cross-border financial services: calling for a financial cybersecurity action task force. In: 19th Annual Security Conference, pp. 1–10 (2020). https://doi.org/10.2139/ssrn.3544325
9. Madnick, S., Johnson, S., Huang, K.: What Countries and Companies Can Do When Trade and Cybersecurity Overlap. Harvard Business Review, 1–6 January 2019
10. Emery, D.: 'My Friend Cayla' Doll Records Children's Speech, Is Vulnerable to Hackers (2017). https://www.snopes.com/news/2017/02/24/my-friend-cayla-doll-privacy-concerns/
11. Levy, A.: Amazon sellers get caught in US-China trade spat as money transfer service abruptly closes (2019). https://www.cnbc.com/2019/02/01/worldfirst-abruptly-closes-us-operations-amid-ant-financial-deal-talks.html
12. Roumeliotis, G.: U.S. Blocks MoneyGram sale to China's Ant Financial on national security concerns (2018). https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7
13. Lockett, J.: Where High and Low Politics Meet: National Security and Cybersecurity. World Economic Forum, 18–21 August 2015
14. Clayton, M.: Exclusive: New thesis on how Stuxnet infiltrated Iran nuclear facility (2014). https://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility
15. Gansler, J.S., Lucyshyn, W., Harrington, L.H.: Defense Supply Chain Security: Current State and Opportunities for Improvement (2012)
16. Huang, K., Madnick, S.E., Johnson, S.: Interactions between cybersecurity and international trade: a systematic framework. SSRN Electr. J. (2018). http://web.mit.edu/smadnick/www/wp/2018-13.pdf
17. Reichert, C.: U.K. cybersecurity agency finds new low-risk concerns with Huawei's security centre (2018). https://www.zdnet.com/article/uk-cybersecurity-agency-finds-new-low-risk-concerns-with-huaweis-security-centre/

18. Vaughan, A.: U.K. government approves Huawei 5G deal despite security fears (2020). https://www.newscientist.com/article/2231678-uk-government-approves-huawei-5g-deal-despite-security-fears/#ixzz6RAbCtYgb
19. Huang, K., Madnick, S.E.: The TikTok Ban Should Worry Every Company, Harvard Business Review, 28 August 2020
20. Ferracane, M., Kren, J., van der Marel, E.: Do data policy restrictions impact the productivity performance of firms and industries? SSRN Electr. J. (2019)
21. Agrawal, A., Gans, J., Goldfarb, A.: A.I. and international trade. In: The Economics of Artificial Intelligence, pp. 463–492 (2019)
22. Aaronson, S.A.: What are we talking about when we discuss digital protectionism? In SSRN (2018). https://doi.org/10.2139/ssrn.3032108
23. Carr, M.: Public – private partnerships in national cyber-security strategies. Int. Aff. **92**(1), 43–62 (2016)
24. Xuetong, Y.: Bipolar rivalry in the early digital age. Chinese J. Int. Politics **13**(3), 313–341 (2020)