A Major Breakdown of International Trade and Next Global Financial Crisis: Could be Caused by Efforts to Prevent Cyberattack on the Web

1st Author
1st author's affiliation
1st line of address
2nd line of address
city, country
phone no., incl. country code
1st author's email address

2nd Author
2nd author's affiliation
1st line of address
2nd line of address
city, country
phone no., incl. country code
2nd E-mail

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," with direct impact on international trade and investment policy. The press has largely focused on trade issues between the USA and China, especially regarding Huawei. But 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 a global phenomenon that needs to be addressed. A taxonomy was developed to understand the different circumstances, actions, and outcomes.

Keywords: Cybersecurity, International Trade, Trade Restrictions, Financial Crisis, Cyberattack

1. Introduction and Motivation

Headlines like "A cyberattack could trigger the next financial crisis, new report says," [1] and "How a Cyberattack Could Cause the Next Financial Crisis," [2] should be of concern to all of us and be important incentives to do something! You probably have not yet heard the ironic headline, "Efforts to Prevent Cyberattacks Could be the Cause of the Next Global Financial Crisis." But, that is already a problem that is emerging and needs to be given serious attention.

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 also be tools for spying and other malicious activities. Hence cybersecurity has increasingly been invoked from the perspective of "national security," with direct impact on international trade and investment policy [3,4,5,6].

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 to exclude from import 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 is a questionable country?

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.

Furthermore, from the digital supply chain perspective, 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]. Most recently, we have seen effects to restrict or ban web services such as TikTok and WeChat.

2. 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 part of our research investigation [9], we identified at least 33 cases, which involved 19 countries as shown in Figure 1.

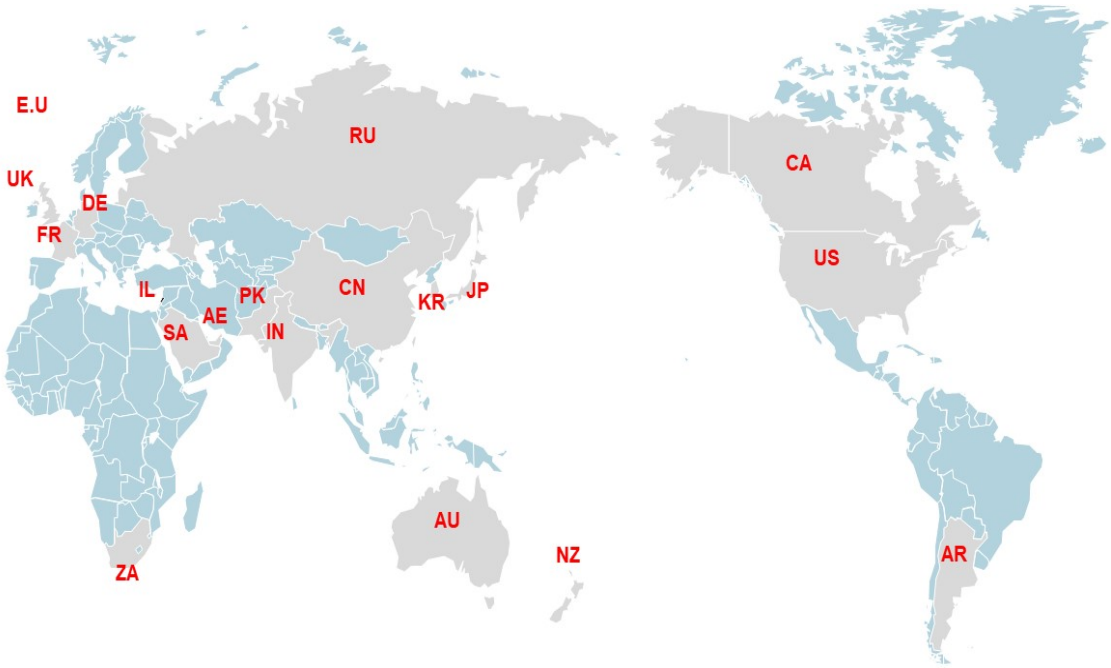

Fig 1: Countries that instituted international trade restrictions due to cybersecurity concerns

When these cases are studied, a complex web of impacts quickly becomes clear, as shown in Figure 2. The point is that, even at this rather early stage, this is already a worldwide phenomenon, and growing.

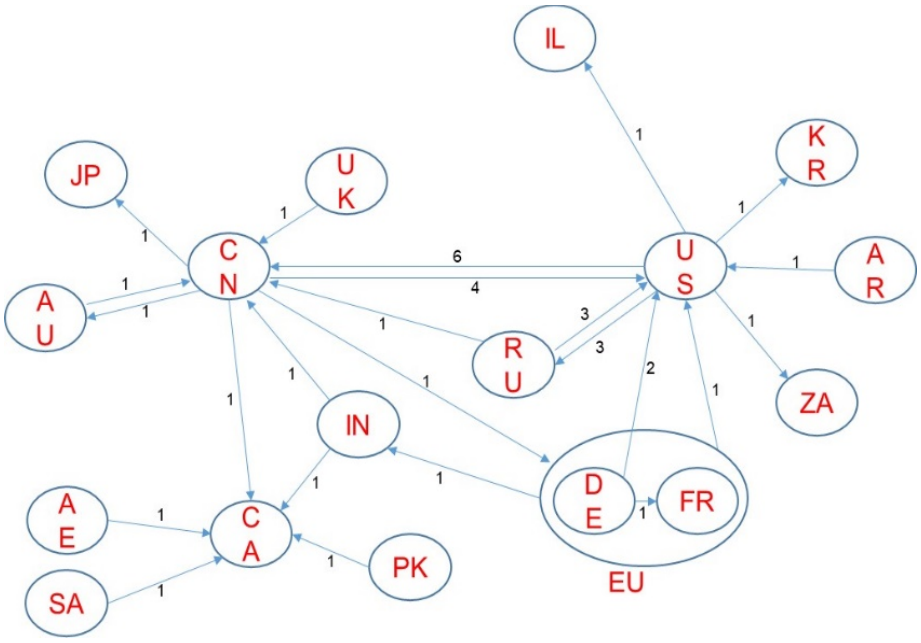

Fig 2: Network Diagram of Countries with international trade restrictions due to cybersecurity concerns

In Figure 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.

As just one example, 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 is 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]

3. Framework for Studying Cybersecurity Impact on International Trade

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

The definition of national cyber security is often intentionally vague to achieve some operating space [13], 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.

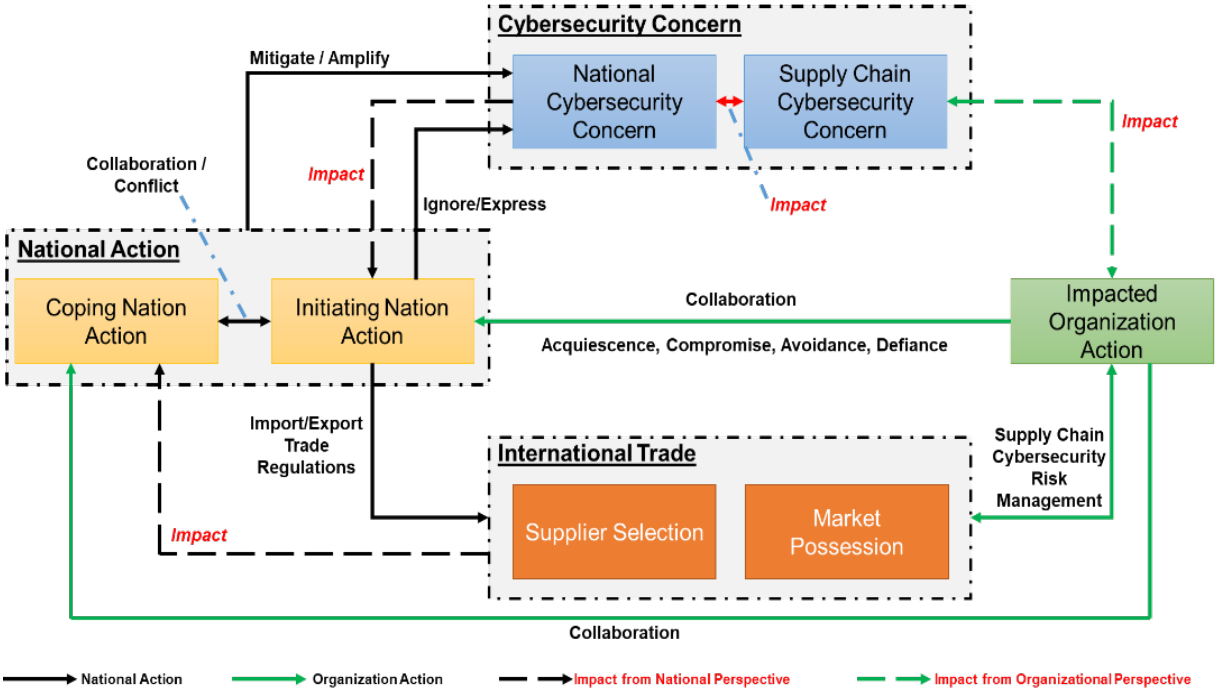

Fig 3: Framework for the Impact on Cybersecurity Concern on International Trade

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 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.

4. Different Actions and Outcomes Possible

There are many different circumstances, leading to differing actions and outcomes. Using the framework above, the actors, actions and impacts for each of the case 33 cases studied are been studied by us 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 check mark with yellow marker are shown whenever the circumstances, actions, and outcomes apply. The important thing to note is that even with this rather small sample of cases, there is a wide variety of cases and actions. The reader is referred to [16] for the details.

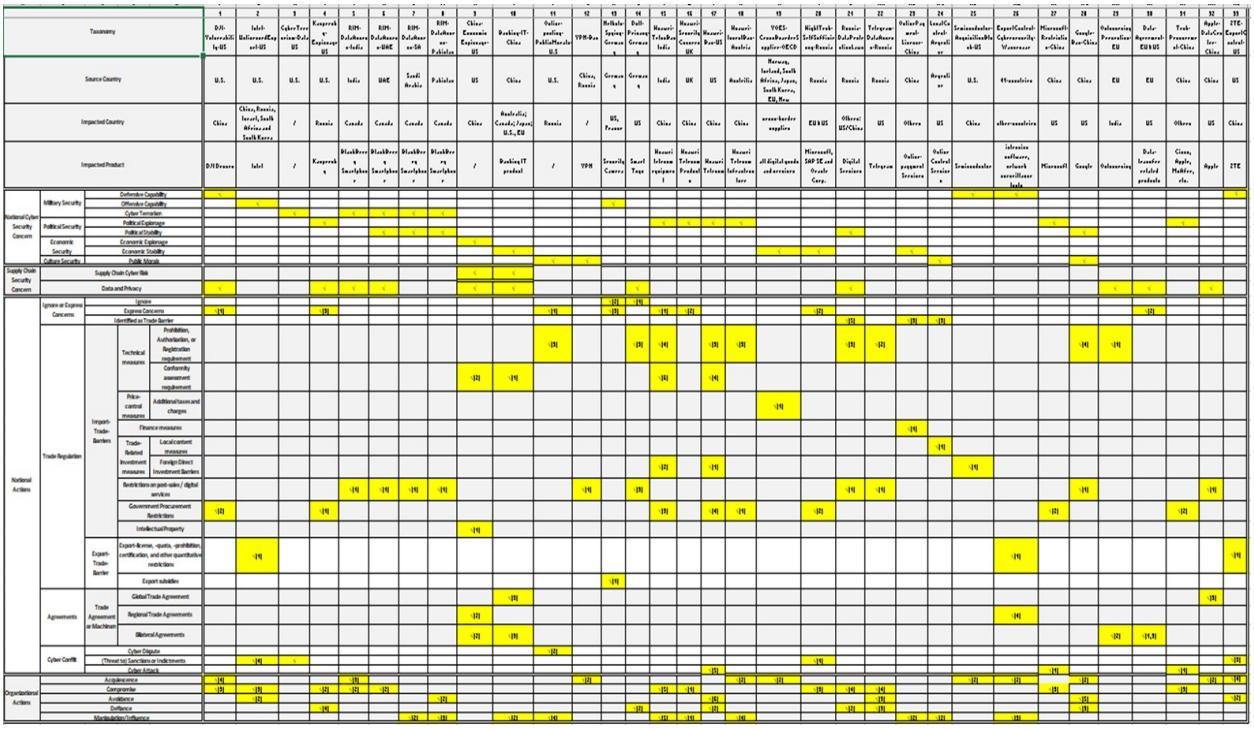

Fig 4: Matrix Listing the Cases Studied and their Differing Circumstances, Actions, Outcomes

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 differing 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 IT 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 largely "exit the US Market".

On the other hand, in 2010, Huawei opened its Cyber Security Evaluation Centre in the UK. "The new Cyber Security Evaluation Centre is a key part of Huawei's end-to-end global security assurance system. This centre 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 UK, 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 UK 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 UK national security from Huawei's involvement in the UK'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 "UK government approves Huawei 5G deal." [18]

From this example we can see that sometimes if the organization can work with the countries and systematically implement the best practices, it could reshape the international trade.

5. 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 following impacts on the economy, the US 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 to not see history repeated.

6. 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 a 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.

References

[1] Bob Pisani, 2018. A cyberattack could trigger the next financial crisis, new report says. CNBC, https://www.cnbc.com/2018/09/13/a-cyberattack-could-trigger-the-next-financial-crisis.html.

[2] Paul Mee and Til Schuermann, 2018. How a Cyber Attack Could Cause the Next Financial Crisis, Harvard Business Review, https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis.

[3] Friedman, A. A. (2013). Cybersecurity and Trade: National Policies, Global and Local Consequences. Brookings Institution Center for Technology Innovation, (September), 1–18.

[4] Kshetri, N. (2016). Cybersecurity-Related Barriers to International Trade and Investment. The Quest to Cyber Superiority. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809819

[5] Mata, D. C. (2015). Cybersecurity Dimensions of National Security. Journal of Law and Administrative Sciences, 132–142.

[6] Farrell, H., & Newman, A. L. (2020). Choke Points. Harvard Business Review, (February).

[7] Lambach, D. (2019). The Territorialization of Cyberspace. International Studies Review, 1–25. https://doi.org/10.1093/isr/viz022

[8] Huang, K., & Madnick, S. E. (2020). Cyber Securing Cross-border Financial Services: Calling for a Financial Cybersecurity Action Task Force. In 19th Annual Security Conference (pp. 1–10). https://doi.org/10.2139/ssrn.3544325

[9] Madnick, S., Johnson, S., & Huang, K. (2019). What Countries and Companies Can Do When Trade and Cybersecurity Overlap. Harvard Business Review, January, 1–6.

[10] David Emery, (2017), 'My Friend Cayla' Doll Records Children's Speech, Is Vulnerable to Hackers, https://www.snopes.com/news/2017/02/24/my-friend-cayla-doll-privacy-concerns/

[11] Ari Levy, (2019), Amazon sellers get caught in US-China trade spat as money transfer service abruptly closes, https://www.cnbc.com/2019/02/01/worldfirst-abruptly-closes-us-operations-amid-ant-financial-deal-talks.html

[12] Greg Roumeliotis, (2018), U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns, 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] James Lockett. (2015). Where High and Low Politics Meet: National Security and Cybersecurity. WORLD ECONOMIC FORUM, (August), 18–21.

[14] Mark Clayton, (2014), Exclusive: New thesis on how Stuxnet infiltrated Iran nuclear facility,

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. (2012). Defense Supply Chain Security: Current State and Opportunities for Improvement.

[16] Huang, K., Madnick, S. E., & Johnson, S. (2018). Interactions Between Cybersecurity and International Trade: A Systematic Framework. SSRN Electronic Journal, (November). http://web.mit.edu/smadnick/www/wp/2018-13.pdf

[17] Corinne Reichert, (2018), UK cybersecurity agency finds new low-risk concerns with Huawei's security centre, https://www.zdnet.com/article/uk-cybersecurity-agency-finds-new-low-risk-concerns-with-huaweis-security-centre/

[18] Adam Vaughan, (2020), UK government approves Huawei 5G deal despite security fears, https://www.newscientist.com/article/2231678-uk-government-approves-huawei-5g-deal-despite-security-fears/#ixzz6RAbCtYgb