Examining How Globalization Through the Technological Industry Has Affected Cybersecurity

Jade Goodwin
INR4931: Globalization
April 19, 2024

Introduction

Over the recent 30 years, the use of the internet and digital technology has only increased. From cell phones, to laptops, to artificial intelligence that can respond to you as if you are conversing with another huma being, the rapid growth of technology and its accessibility seems to be never ending. Everywhere you go, each person around you has some kind of technological device in their hands or at their waist. From an international relations perspective, although technological advancements are a prodigious thing, there are also a consequential security risks associated with it. Cybersecurity has become an up-and-coming field that is necessary to every functioning government and company. Since the dissemination of the internet in 1993, there have been occurrences and risks of cyberattacks and cybercrimes.

Despite the growing significance of cybersecurity in the era of globalization, there remains a notable absence of comprehensive research investigating the relationship between these two phenomena. This leads us to my research question: How has globalization, through the spread of technology, affected cybersecurity? This study intends to bridge this gap by

scrutinizing the link between globalization and cybersecurity, with a particular focus on the United States for empirical evidence. Furthering the research, I used two other studies, "Cybersecurity in the Global Economy" by Aidan Keena and "Cyber Security Risks in Globalized Supply Chains: Conceptual Framework" by Shipra Pandey and Rajesh Kumar Singh. Keena's article discusses the historical trajectory of cyberattacks, highlighting their severity alongside technological advancements from globalization. In contrast, Pandey and Singh's work observes the vulnerability of global supply chains to cyber threats imposed by the interconnected globe. While existing research lacks qualitative data of cybersecurity and its relationship to globalization, this study seeks to strengthen these ideas with empirical evidence. By analyzing longitudinal data on U.S. technological trade exports and reported cyberattacks from 2012 to 2023, I aim to uncover a quantitative relationship between technological globalization and cybersecurity threats.

Literature Review

While there has not yet been a lot of research done which examines the relationship between globalization and cybersecurity, I chose “Cybersecurity in the Global Economy” written by Aidan Keena and, “Cyber Security Risks in Globalized Supply Chains: Conceptual Framework” written by Shipra Pandey and Rajesh Kumar Singh.

The first article discusses a brief history and chronological sequence to the current prevalence of cyberattacks, beginning with the advent of the internet. It argues that cyberattacks have become much more harmful and prevalent over the past 30 years with the rise of and spread of technology. More importantly, while rapid technological advances have allowed for

unprecedented levels of productivity, they have also rendered our most critical systems seriously vulnerable to disruption (Keena, 2024). As a research example, the article dives into a case study surrounding the 2021 Colonial Pipeline Company's where they were blackmailed via computer hacking into paying $4.4 million in cryptocurrency to prevent disruption and leak of sensitive company information. On top of physical infrastructure, cyberattacks and cybercriminals also have the capability of financial institutions, completely wiping out records of assents and financial statements. The example used to discuss financial risks of cyberattacks was the New Zealand stock market fiasco during primitive DDoS attacks.

Ultimately, the first article does not use enough statistical data to hold internal validity, as it is solely based on a limited number of case studies. It goes into potential solutions for the future, including implementing mandatory malware and digital laws. It mentions China as one example, since they are the sole internet service provider for their country, making it much safer from global affects. While this article has shown that cybersecurity threats are on the rise and increasing, it does not effectively present a potential reasoning for what is causing its rise. The focus of their study seems to examine the current state of global cybersecurity and its potential effects on G20 and other countries of the global north. It fails to examine the correlation between the rise in cyberattacks and technological globalization.

The second article examines cybersecurity risks on global supply chains, as well as risk mitigation strategies adopted by the SCs. The methodology of this research is through five specific case studies: Tesco Bank (2016), Leoni AG (2016), Hyundai and Kia Cars (2016), German steel manufacturer (2014), and Wannacry Ransomware (2017). There are operational, supply, and customer risks demonstrated by these case studies, which signify the close relationship between supply chains and potential cyberattacks. Cyberattacks on global supply

chains have the potential to disrupt supply and operational function of the branches of the companies in multiple states (Pandey and Singh, 2021). They argue that with increased digitization of global markets, global supply chains are more likely to fall risk to cyberattacks and potential disruption.

Although current research on this topic can support a close relationship between a rise in cyberattacks/cybercrimes and the spread of technology through globalization, much of it fails to offer or examine empirical evidence. While case studies can be helpful, empirical evidence is needed to offer larger sample sizes as well as statistical analysis to determine correlation between the variables. Furthermore, while it is beneficial to look at cases of cyberattacks on companies, it can be too specific of a scope, since it fails to examine cyberattacks on individuals as well as on governments.

Overall, the biggest risk associated with current research surrounding my topic is the use of empirical data over the use of case studies. There is a lack of statistical comparison which can provide evidence to the relationships between the rise in technology caused by globalization and the increase in cyberattacks/cybercrimes. The current methods of research also focus too heavily on the cybersecurity aspect alone, and less on it's relationships with technological globalization. It is important to consider measures of globalization when comparing it to the cyberattacks, not just through company cases or supply chains. Trade is one of the best measures of globalization, as it represents not only the relations and connections of goods and services between states, but also the spread and movement of certain types of goods and services.

Theoretical Argument

The growth rate of the accessibility and the evolution of technology seems to be at a constant rapid increase due to globalization. As of recently, there has been an outburst in the use of generative Artificial Intelligence, which everyone from students, to businesses, to governments use in their day to day to make cyber tasks easier. Generative AI serves as just one example of a technological advancement which can pose a threat to cyber security globally. Threats to cybersecurity and digital grids can have a multitude of detrimental effects both politically and economically on states – specifically, data breaches and DDoS (Distributed Denial of Service) attacks can affect bank records, election polls, personal security, etc. For example, in 2024 alone, more than 45 countries will hold elections which accounts for more than 50% of the world's GDP (World Economic Forum, 2023). Even just four years ago in 2020, there was debate surrounding China's possible interference with the United States presidential election.

The globe has become increasingly interconnected, and a prime link for this is through international and regional trade. Trade is an incredibly significant tool for monitoring and measuring globalization. Since 1995, global trade has increased at an average rate of 4 to 6 percent annually (World Trade Organization, 2022). According to the World Trade Organization, 20% of global trade is digital commerce, and it is projected to increase an additional 5% the following year. It is clear that technology is constantly increasing and advancing each year. Trade in technological goods and services continues to rise, and so does cybersecurity threats along with it. In the Word Economic Forum's 2024 Global Cybersecurity Outlook, around 29% of leaders reported that their organization had suffered from a material impact from a cyberattack within the past 12 months.

The hypothesis of my research study is that as the spread of technology increases over time, there will be a direct relationship to the amount of cyberattacks/cybercrime.

Research Design

In order to examine the relationships between globalization (through the spread and accessibility of technology) and the effects on cybersecurity, I used the United States as an example to test my hypothesis. I chose the United States as an example since it is a country that has a lot of easily accessible data, and it also is very active in terms of trade and international relations, which are both representations of globalization. In 2023, the United States was the second top exporting country globally, falling behind China (Statista, 2024). The United States is also involved in many international organizations such as the WTO, NATO, the UN, etc. To test my hypothesis, I examined the U.S. Trade Exports of Technology from 2012 to 2023 (of both goods and services) as my independent variable and reported cyberattacks in the United States in the form of data breaches from 2012 to 2023 as my dependent variable.

The importance of examining U.S. Trade Exports of Technology over the span of 11 years is to grasp the measure of globalization of technology. The significance in comparing the independent variable to the amount of reported data breaches is to compare the relationship between the growth of technological globalization with the occurrences of cyberattacks/cybercrime. In order to compare the two variables, I first examined each one individually over the course of 11 years from 2012 to 2023 and plotted the data using Excel. I used data from Consensus.gov to determine the amount of technological exports per year (Figure 1) and Statista.com to determine the amount of reported data breaches per year (Figure 2). After

plotting the data of each variable over the 11-year span, I used a statistical regression plot in Excel in order to compare the correlation of the variables (Figure 3).

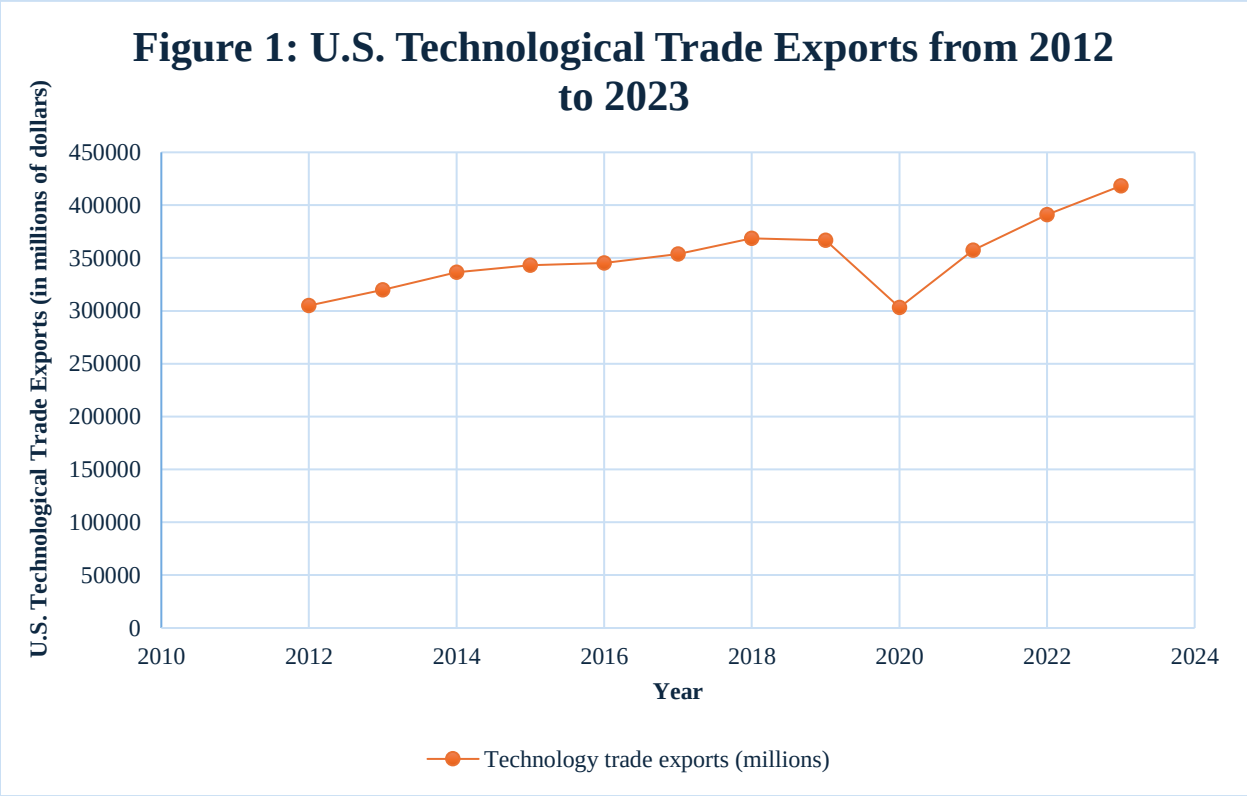


Figure 2: U.S. Data Breach Cases from 2012 to 2023

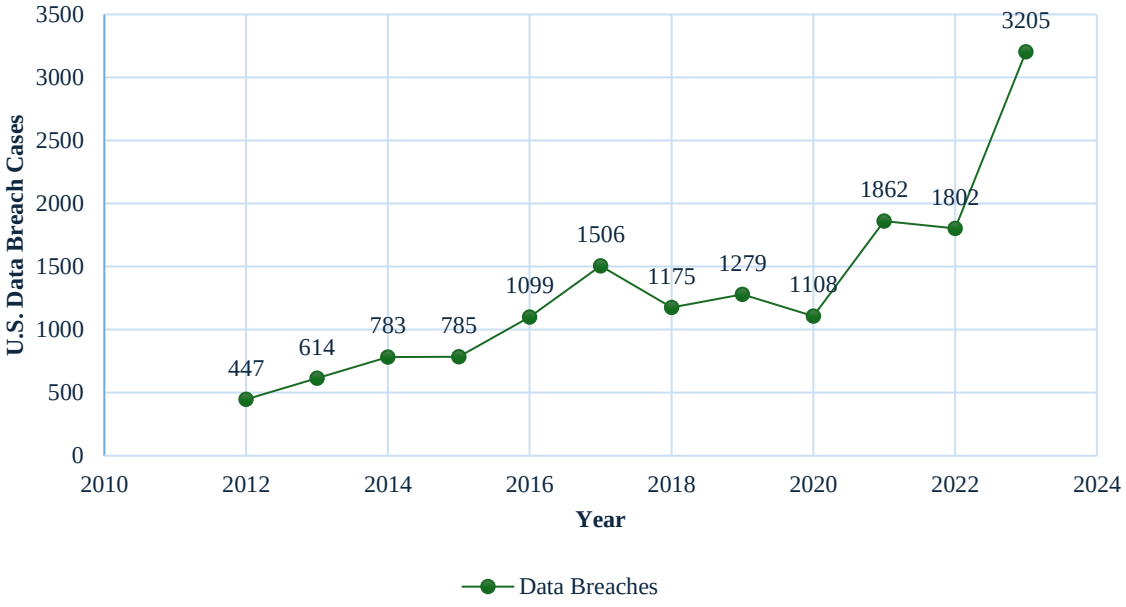
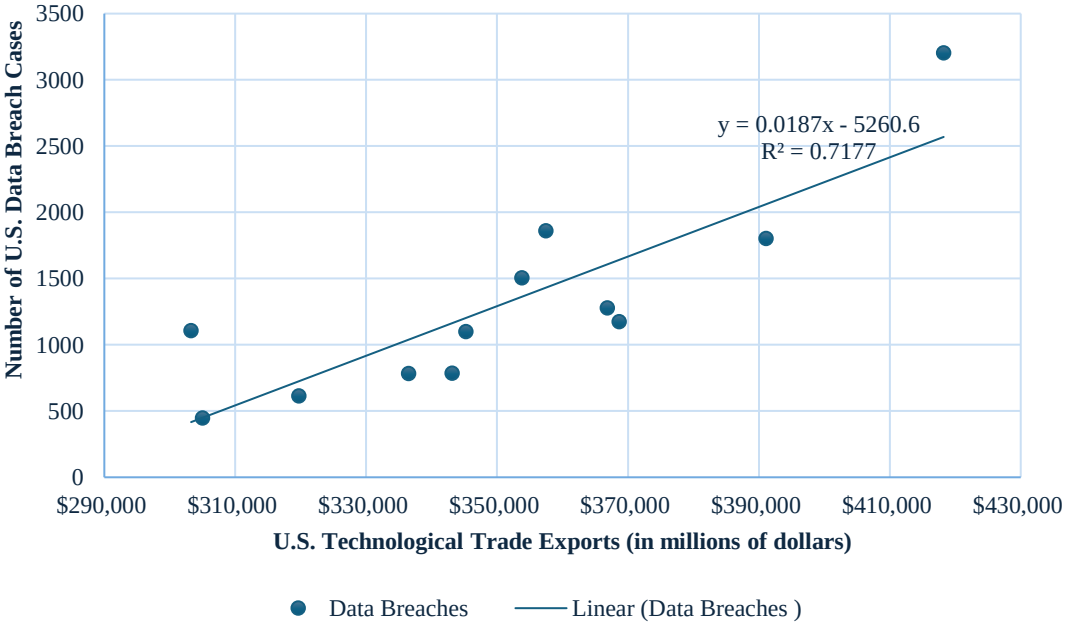


Figure 3: U.S. Data Breaches Compared to Technological Trade Exports



Findings

As shown in figure 1, the U.S. technological trade exports (in millions of dollars) for each year had almost a completely steady increase, aside from the dip in years 2018 and 2019 which can assumably be contributed to repercussion of the COVID-19 pandemic. In figure 2, the trend in data breach reports seem to be very similar compared to the trend of technological trade. From 2012 to 2023 there is practically a steady increase, aside from 2018 to 2019 which can be attributed to COVID-19, and then another small dip from 2021 to 2022.

When comparing the two variables together (Figure 3), you can see that there is a positive linear relationship between the amount of U.S. technological trade exporting and reported data breaches. The r-squared value of 0.7177 can suggest that there is a strong correlation between the variables. Thus, it can be inferred that as the amount of technological trade in exports increases, so does the occurrence of data breaches, and vise versa. While much more in-depth study is needed to investigate causation, there is definitely a correlation between the two variables.

The uncovered relationships in the graphs support my hypothesis that as the spread in technology as a result of globalization increases, there is also an increase in cyberattacks/cybercrimes. There is a strong positive linear relationship between the two values. As the United States continues to export more and more technological goods and services, there is a continual rise in the amount of cyberattacks that occur. Overall, my research can support that the increase in technological accessibility and advancements caused by globalization is increasing the need for cybersecurity; there is a correlation between it and the rise of cyber-attacks.

Conclusion

In conclusion, this study sheds light on the intricate relationship between globalization, t technological advancement, and cybersecurity. Over the past three decades, the proliferation of digital technology has altered the global landscape. Alongside these advancements there are significant security vulnerabilities, with cyberattacks posing a serious threat to governments, businesses, and individuals worldwide. Although the increase in cyberattacks globally has continued alongside technological globalization, existing research has often overlooked the relationship between the two phenomena. By analyzing trends in U.S. technological trade exports and reported cyberattacks from 2012 to 2023, we uncover a compelling correlation between the proliferation of technology and the incidence of cyber threats. Our findings highlight the need for cybersecurity measures in an increasingly interconnected world, in which the consequences of cyberattacks extend past economic ramifications to political and societal repercussions. Moving forward, it is necessary for policymakers, businesses, and cybersecurity experts to collaborate in devising proactive strategies to mitigate cyber risks. As technological advancement continues, the need for effective cybersecurity measures becomes more significant; there is an urgency for greater research and action in this critical global sector.

Bibliography

Bonnett, E. (2020, July 7). *Technology trends are reshaping trade*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/technology-trends-are-reshaping-trade/#:~:text=A%20report%20by%20Japan%E2%80%99s%20Ministry%20of%20Economy%2C%20Trade

Foreign Trade Data Dissemination Branch. (2019). *Foreign Trade - U.S. Trade with Advanced Technology Products*. Census.gov. https://www.census.gov/foreign-trade/balance/c0007.html

Global Cybersecurity Outlook 2024 J A N U A R Y 2 0 2 4 In collaboration with Accenture. (n.d.). In *weforum.org*. Retrieved April 25, 2024, from https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Keenan, A. (n.d.). *CYBERSECURITY IN THE GLOBAL ECONOMY*. Retrieved April 25, 2024, from https://static1.squarespace.com/static/612fdeb8ae0c5815484a61c9/t/61db89d68bc0bb15e77862c2/1641777623117/G20_1.pdf

Pandey, S. (2019, October 21). *Journal of Global Operations and Strategic Sourcing | Emerald Insight*. Www.emerald.com. https://www.emerald.com/insight/publication/issn/2398-5364

Petrosyan, A. (2023, April 1). *U.S. data breaches and exposed records 2018 | Statistic*. Statista; Statista. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Top exporting countries 2023. (n.d.). Statista. Retrieved April 25, 2024, from https://www.statista.com/statistics/264623/leading-export-countries-worldwide/#:~:text=The%20value%20of%20exports%20of%20China%20amounted%20to

World Economic Forum. (n.d.). World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

World Trade Organization. (2022). *WTO | Evolution of trade under the WTO: handy statistics*. Www.wto.org. https://www.wto.org/english/res_e/statis_e/trade_evolution_e/evolution_trade_wto_e.htm

Appendix