M.A. in Political Science
with a Concentration in European Union Policy Studies
James Madison University

Under Attack: Trading Digitally in the Age of Vulnerability

Annabelle C. Giaccone

Abstract

The rise in digitalization has sparked the Fourth Industrial Revolution, raising new concerns and deep divisions throughout the European Union (EU). While the adoption of the Digital Single Market Strategy on May 6, 2015 attempted to adapt to the increasingly digital world, it further highlighted differences among Member States. This paper argues that cross-national variations in digital trade restrictiveness can be explained by the number of cyber-attacks a Member state experiences. This study differs from existing explanations in that it takes a technological perspective and attempts to explain a digital question with a digital phenomenon. The paper tests this hypothesis through a combination of anecdotal and quantitative evidence. Anecdotal evidence regarding the evolution of cyber-attacks in France in Germany suggests that both countries responded to cyber-attacks with strict national legislation towards digital issues. A simple linear regression of the number of cyber-attacks on a country's Digital Trade Restrictiveness assesses the magnitude of the relationship between these variables for a sample of 28 EU Member States. While the data suggests a causal relationship between the two variables, further research is required to provide a more complete explanation for the variation in question.

Written for Topics in Economic and Social Policy (Dr. Helen Callaghan)
Presented at James Madison University – Max Weber Programme Graduate Symposium,
EUI, Fiesole, Italy 12 April 2019.

Introduction

The Fourth Industrial Revolution – motivated by rapid technological change and digitalization – has already had a strong impact on global trade, economic growth and social progress. Cross-national e-commerce has generated trillions of dollars in economic activity in recent years and continues to accelerate. The ability of data to move across borders supports new business models, boosting global GDP by 10% in the last decade alone. It has facilitated the use of blockchain technology, thereby increasing efficiency and transparency in international trade (World Economic Forum 2018). However, digital trade barriers, including outdated regulations, fragmented governance and strict data localization policies, could potentially prevent these gains from fully materializing. At the same time, policy-makers must balance societal concerns in the digital commercial space while stakeholders need to navigate different divergent national responses.

Today, many of the existing global trade rules do not reflect this new reality and are not easily transferred to the digital era. New technologies and business models raise new governance questions and challenges. In the absence of global rules, governments move unilaterally to regulate their domestic markets. The risk of fragmentation materializes, which increases the barriers for large and especially small companies to operate internationally. The emergence of digital trade barriers has resulted in fragmented and inconsistent approaches to the digital sector which inherently limits progress towards the completion of the Digital Single Market.

The importance of digital trade and the need to secure free cross border flow of data, create rules on e-commerce and address data privacy issues are widely recognized. In the "Trade for All" Communication of October 2015, the European Commission refers to the digital revolution, describing digital trade as an offensive interest for the European Union (EU), creating many opportunities for companies including small-to-medium enterprises (SME) and consumers. A digital trade strategy will reinforce this position further (Business Europe 2017). It is due to this limitless potential which emerges through a freely interconnected world that divergences among EU Member States become increasingly relevant. Without consensus on the issue, the EU will lag behind powerful countries such as the United States (U.S.) and China. In addition, as Europe's population continues to age, the prevalence of the digital world becomes more apparent. The digital revolution provides not only increased labor opportunity in European countries but also an increased potential for jobs to be performed remotely, a characteristic highly compatible with an aging population. Therefore, variations among Member States creates inconsistencies and require a critical examination in order to prevent economic damage.

This paper seeks to explain cross-national variations in the levels of digital trade restrictiveness. This paper proposes that cyber-security attacks can explain variations among Member States levels of digital trade restrictiveness. Digital trade restrictiveness can be defined as, the level of which a country is open or closed to participating in digital trade practices (DTRI 2018). I hypothesize that if a country has a higher number of cyber-attacks, then a Member state's digital trade policies will be more restrictive.

This analysis uses two case studies which exemplify the trend the original hypothesis put forward. A simple linear regression was conducted using data on a country's number of cyber-attacks in the year 2018 and the Digital Trade Restrictiveness scores from the 2018 Digital Trade Restrictiveness Index. The paper proceeds as follows: section two provides a background on the evolution of cybersecurity, the digital single market and the digital single market strategy.

Section three gives an overview of the existing literature on this topic. Section four explains the divergences which is followed by a case study analysis for two Member States. Section five provides a methodology outlining the process of the conducted study followed by a results section. The conclusion summarizes the findings and makes suggestions for further research.

Background

The Digital Single Market

Before delving into the literature, it is important to provide a definition of the Digital Single Market (DSM) to provide context for the research question being analyzed. According to the European Commission, The Digital Single Market is a policy belonging to the European Single Market that covers digital marketing, e-commerce and telecommunications. The DSM is part of the Digital Agenda for Europe 2020 program of the EU, an initiative of Europe 2020 proposed strategy. It is defined by a Digital Single Market Strategy for Europe by the European Commission (2015).

The Digital Single Market Strategy

Citizens and businesses of the EU have often faced barriers when using online tools and services. These barriers mean that consumers have restricted access to some goods and services, businesses cannot reap all benefits from digitalization and governments and citizens cannot fully benefit from this digital transformation. The DSM Strategy was adopted on May 6, 2015 and is comprised of three policy pillars: improving access to digital goods and services, creating an environment where digital networks and services can prosper and using digitalization as a driver for growth (Cousiel 2019).

The Evolution of Cybersecurity

The evolution of cybersecurity in the EU is important when evaluating its relationship to the digital trade sector. By examining supranational responses to cybersecurity issues, the disparities in national policies become more visible. The term cyber and its associated terms cyberspace and cybersecurity have drifted from the world of the arts and into the mainstream. A cyber-attack is a deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft (European Network and Information Security Agency 2015). As technology has continued to advance, cybersecurity concerns have become increasingly prevalent for the EU. On October 18, 2018, the European Council called for measures to build strong cybersecurity in the EU. EU leaders referred in particular to restrictive measures able to respond to and deter cyber-attacks.

An important EU response to the cybercrime phenomenon is the General Data Protection Regulation (GDPR). This data protection regulation consists of 11 chapters broken down into 99 articles covering the rights of data subjects (people rising in the territory of the EU); the responsibilities of the controllers and processors of data; transfers of personal data to third countries or international organizations; the actions of independent supervisory authorities and the applications of remedies, liabilities and penalties (European Commission 2016). The regulation clarifies what constitutes personal data. This includes name, address, localization, online identifier, health, income information, cultural profile and other personal characteristics.

(See Figure 1.) Under GDPR, all citizens residing in an EU country have a right to access their personal information and also secure the right to erasure, commonly known as "the right to be forgotten" (E-Trade 2018).

The current literature suggests alternative explanations for the factors that influence variations in digital trade restrictiveness. These explanations include The Digital Divide, National Sovereignty and Digital Endowments. The following brief review of these explanations shows that there is a gap in research concerning the role of cybersecurity issues in relation to digital trade policies.

Literature Review

A significant portion of the research on this subject suggests socio-economic and accessibility factors as the primary reasoning for variations across countries. Commonly referred to as the Digital Divide, this concept emphasizes access to fundamental information technologies – most often telephone and internet access. Wong, a professor at the Lee Kuan Yew School of Public Policy, evaluates the divide in Asian countries based on penetration levels of telephone main lines, PCs, and Internet use. In 2001, the Organization for Economic Cooperation and Development (OECD) defined the term 'Digital Divide' as "the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard to both their opportunities to access information and communication technologies (ICT) and to their use of the internet for a wide variety for activities" (2002). The Digital Divide has two main aspects: the first gap considers mainly the division between those who have access to ICT such as computers and the Internet and those who do not. This type of scope often refers to the urban-rural divide, the latter having lower internet speeds, prices and technological choices. The second gap refers to different types and levels of internet use, motivation and skills: looking at what uses, and benefits people enjoy, once they have access to the internet (Negreiro 2015).

Many developments have already been made which have further exaggerated the Digital Divide. The U.S. and a number of leading digital nations are backed by the vast lobbying power of Silicon Valley and big business. On the other side, a number of emerging and developing countries are looking to resist new rules that they perceive as adding extra burden on them, with vague benefits. The introduction of the "Digital Trade Agenda" during the Obama administration, allowed for this resistance to surface. This agenda was adopted by the Trans-Pacific Partnership (TPP). Many of the less developed countries believe the rules outlined in the agenda will widen the digital divide that already exists between the developed and developing world, by exposing local digital firms to fierce competition. As the history of trade rules has shown, rapidly opening developing economies up to foreign competition can potentially hollow them out. In addition, some countries argue that they need to adopt more active policy to develop their own digital economies, which they fear global rules could limit (The University of Manchester 2019).

The alternate explanation identified within this strand of the literature considers the ability or inability of citizens in a certain country to access technology as well as the fear of exploitation in developing countries. While this socio-economic perspective highlights further issues concerning the digital sector within the EU, it has an inherent focus on the individual rather than the state as a whole.

The National Sovereignty argument says that the prioritization of maintaining certain competencies at the national level has a significant effect on a country's willingness to surrender their digital abilities. Sovereignty is defined as "the full right and power of a governing body over itself, without any interference from outside sources or bodies" (Pusterla 2018). In political theory, sovereignty is a substantive term designating supreme authority over some polity (Pusterla 2018). The concept of national sovereignty has been utilized to explain divergences in digital trade restrictiveness. Viviane Reding, a Luxembourg politician and former Member of European Parliament (MEP), attributes fragmentation to 'national silos.' Her sovereignty concerns surround the idea that digital sovereignty should be held at the European level. She states,

> "Now that we still have the economic power we should use this potential to determine our own norms. This implies acting together, based on our European values, anticipating future developments by embracing technology and innovation and negotiating with our international partners on a legal level playing field, enabled by a coherent and strong European policy" (2015, 3).

On the opposing side of the sovereignty debate, there are scholars who argue that national sovereignty is threatened by digitalization and should be avoided. In the book, "Twilight of Sovereignty: How the Information Revolution is Transforming Our World." The author, Walter Wriston, tackles the concept of sovereignty in the "Age of Information." He states, "[s]overeignty, the power of a nation to stop others from interfering in its internal affairs, is rapidly eroding." Many forces today, such as trade, global capital flows, and environmental degradation are thought to undermine sovereignty. Wriston argues that the developing conventional wisdom seems to be that the Internet is contributing to the erosion of sovereignty and will, perhaps more than any of the other globalization forces, contribute to relegating sovereignty and its traditional trappings to the other irrelevant aspects of history (Wriston 1998).

The third perspective that emerges is one that discusses the age of digitalization as a tool to strengthen sovereignty. Perritt argues, that the Internet has the potential to strengthen national and global governance – thus enhancing sovereignty rather than destroying it. From the perspective of national governance, the Internet can be harnessed to promote the Rule of Law, which is critical for good governance of societies all over the world (1998). These opposing views have contributed to the divergence on the issue of digital trade within the EU. Although the sovereignty debate introduces polarizing perspectives, there is substantial literature which suggests the sovereignty issue can explain digital strategy variations.

Similar to the socio-economic theory, digital endowments are another explanation thought to influence variations in strategy, but this theory focuses on the state as a whole whereas, socio-economic focuses on the individual. Digital Endowments are introduced as the third explanatory factor that is thought to have a causal relationship with variations in digital trade strategies. Members of the EU have different positions on matters of digital openness, and those differences typically reflect the role of the digital sector in national economies and the relative size of digital endowments. For instance, countries with smaller digital endowments (e.g. digital infrastructure like networks) often believe they do not stand to gain as much from digitalization as countries with larger endowments. Fredrik Erixon Philipp Lamprecht argues that this is a misconception. He states, "It is crucial to note that economic success in the digital

economy is actually not merely the absolute level of digital endowments, but rather the way in which these endowments are effectively employed" (2018).

There is a long history of analysis about why countries tend to be more or less open to reforms that increase trade and competition. While there is a pattern throughout history that smaller countries generally are more open than larger countries, it is equally clear that the size of a country's "endowments" – in this case, the relative size of digital endowments like digital infrastructure or digital human capital – informs policy choices. In other words, positions of openness tend to favor those factors of production that are in abundance and harm production of factors that are scarce and vice versa (Rogowski 1990).

While this survey of the literature has successfully explored the evolution of cybersecurity and the suggested explanatory factors that create variations in digital trade restrictiveness, the connection between the two fails to be adequately represented. The existing literature explicitly identifies that a digital divide exists and that the threat of cybersecurity is growing rapidly, but there is no indication that the cybersecurity phenomenon could be responsible for the divisions and variations among the EU Member States. This paper contributes to the literature in that it bridges the gap between ambiguous explanations for digital trade variations and cyber threats. It proposes a new way of explaining the disconnect being experienced in the digital sector of the EU. In addition, this paper focuses specifically on the EU Member States and creates the empirical puzzle of why countries who are sufficiently similar in that they have all successfully acceded into the EU, ultimately have variations among them in a sector that has largely been regarded as positive and potentially revolutionary. In sum, the research examined in this review is preliminary and fragmented. While all of the research concludes that variations exist, the findings have significant vulnerabilities in that they fail to explain a digital problem with a digital phenomenon.

Divergences

In a political entity like the EU, it is puzzling how countries who are supposed to share common values yet maintain stark differences are able to cooperate so closely. This is particularly true for the growing Digital Sector in the EU. At the Tallin Digital Summit in September 2017, Commission President, Jean-Claude Juncker stated,

> Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and responses to cyber-attacks. We do not want to be the weakest link in this global threat (European Commission 2017).

At this point, it is clear after observing the literature that variations among Member States exist and there have been numerous attempts to explain why these variations exist. By emphasizing the areas of the digital sector where Member States tend to have significant divergences, a better understanding of these disparities can be acquired and will assist in the explanation of cyber-attacks as an explanatory factor.

While the EU has made good efforts to improve the policy conditions for digital goods and services, the policy fragmentation in Europe and the severity of some of the restrictions in place create "thick" digital borders. In Europe, the two most digitally restrictive countries are

France and Germany (DESI 2018). Both countries have more restrictive digital trade policies than most other developed countries. France is also the only European country that is a part of the Top Ten most restrictive countries in digital trade worldwide (DTRI 2018). On the other end of the spectrum, Ireland, Norway, Malta, the Netherlands, Latvia, Luxembourg and Estonia rank high in digital openness. The restrictive culture of France and Germany is very different from the digital openness of a country like Ireland. Their restrictive stance has often prevented the EU from making fast progress to create a DSM. Following Brexit, France and Germany will be the two dominant EU economies. Their influence in the EU will, therefore grow, which is likely to make it more difficult to advance the DSM (DTRI 2018).

In terms of where the divergences exist, the most significant factor that has defined these variations among Member States' digital strategies is data localization policies. Some countries, such as Finland have very relaxed data localization policies. According to the Information Technology and Innovation Foundation, "Finland's Account Act (1997) requires that a copy of companies' accounting records be stored in Finland. Alternatively, the records can be stored in another EU country if a real time connection to the data is guaranteed" (Cory 2017). Finland is an example of a country that does not have high restrictions in their digital trade strategy. However, this does not hold true for the previously mentioned countries, Germany and France. Germany, along with France, has been at the center of efforts to force companies to store data only in Europe or even in-country, such as through a "Bundescloud" (a cloud for government data) in Germany. Belgium, similar to Finland has a less restrictive approach. Belgium's laws require accounting and tax documents to be kept in office, agency, branch or other private premises of the taxpayer where they have been kept, prepared or sent. Companies can apply to Belgian tax authorities for an exemption to this requirement. These accounting records may be kept in another place (such as overseas), provided that immediate access to the records can be granted or that such records can be provided on short notice (Cory 2017).

This presentation of the divergences among Member States shows that even similar countries in terms of economic development and performance have conflicting strategies when it concerns digital trade. In addition to this claim, Germany and France have higher percentages of their populations who experienced cyber-attacks within the past year. By comparison, the percentage of people in Belgium and Finland who experienced cyber-attacks was much lower (ENISA 2018). This aligns with the original hypothesis and prompts further testing on the remaining EU-28.

Examination of the Case Studies

This paper examines two case studies, France and Germany in order to show how their national digital strategies have evolved as cyber-attacks have become more intricate and advanced. These two case studies aim to show how increased cyber-attacks within France and Germany have provoked the formulation of thorough and hard line responses, such as digital restrictiveness, as a mechanism to limit negative effects felt by cybercrime.

Case Study: France

Digital Policies: Pre-attacks

France adopted a data privacy law in 1978. It applied to public and private organization and forbids gathering sensitive data about physical persons (sexuality, political or religious

opinions). The law is administered by the Commission Nationale de l'Informatique et des Libertés (CNIL), a dedicated national administration. Since the implementation of this first Data Protection law, it has been modified twice: in 2004 following the transposition of Directive 95/46 on the protection of personal data and in 2016 following the French digital republic law (Dreyfus 2018). It is important to observe here that the first Data protection law in France actually preceded the invention of the Internet in 1983. While there were modifications made after the implementation of the Data Protection Law, no real or substantial reforms were made in terms of the digital economy until 2016.

Cyber-Attacks

According to Defense Minister Jean-Yves Le Drian, cyber-attacks in France continue to double in numbers with each passing year and their severities have only worsened (BBC 2017). In December 2010, attacks began with an email which was sent around the French Ministry of Finance. The email's attachment was a "Trojan Horse" type consisting of a PDF document with embedded malware. Once accessed, the virus infected the computers of some of the government's senior officials as well as forwarding the offensive email on to others. The attack infected approximately 150 of the finance ministry's 170,000 computers (BBC 2011).

More recently, in 2015, the Paris-based French broadcasting service TV5Monde was attacked by hackers who used malicious software to attack and destroy the network's systems and take all twelve of its channels off the air. Responsibility for the attack was initially claimed by a group called the "Cyber Caliphate." However, a more in-depth investigation by French authorities revealed the attack on the network had links to APT-28, a Russian-affiliated hacker group (BBC 2016).

APT-28 struck again in May 2017, on the eve of the French presidential election, when more than 20,000 e-mails belonging to the campaign of Emmanuel Macron were published on an anonymous file-sharing website (Willsher 2017).

By observing the consecutive and evolving nature of cyber-attacks in France, it can be concluded that with each new attack, the stakes became higher and the consequences worsened. Therefore, the amendments to existing policies and the implementation of new policies calling for increased digital restrictiveness can be seen immediately after these cybercrime events had taken place.

Examining the Policy Response

On October 7, 2016, the French Digital Republic Act came into force following a year long process which began in December 2015 to amend the laws regulating various aspects of the digital economy in France. This law introduced new provisions that regulate the digital economy as a whole (such as open data, online cooperative economy, revenge porn and access to the internet). For privacy professionals, this law was important as it introduced several key amendments under the French Data Protection Act of 1978 and other laws, prior to the GDPR's implementation in 2018. The provisions of the Digital Republic Act are broken down into ten key points. The most significant amendment to the Data Protection Act concerns the French Data Protection Authority's (CNIL) power to impose administrative fines. Previously limited to EUR 150,000 under the amended Data Protection Act, the CNIL is now able to impose fines up to EUR 3 million. The Digital Republic Act explained that once the GDPR came into force in 2018, the CNIL had the ability to impose administrative fines of up to EUR 20 million or 4% of total worldwide annual turnover for any data protection violations as defined under article 83 of the

GDPR. But controllers in France may still be fined up to EUR 3 million for any violation to the amended Data Protection Act that is outside the scope of the GDPR. This is particularly significant in relation to the new rights that are granted to the data subjects (Proust & Goossens 2016). Given that we see a massive increase in the amount of cyber-attacks in 2015 and 2016 in France, the policy responses to the digital economy such as The Digital Republic Act and modernized data protection laws can be considered timely and strategic rather than coincidental.

Case Study: Germany

Digital Policies: Pre-attacks

In the early 1960s, consideration for comprehensive data protection began in the U.S. and further developed with advancements in computer technology and its privacy risks. Therefore, a regulatory framework was needed to counteract the impairment of privacy in the processing of personal data. Germany was one of the first countries with the strictest and most detailed data privacy laws in the world. The citizens' right to protection is stated in the Constitution of Germany, in Art. 2 para. 1, and Art. 1 para 1. (Deutscher Bundestag 2017). German citizens' data is mainly protected under the Federal Data Protection Act of 1977 or Bundesdatenschutzgesetz (BDSG), which has been amended most recently in 2009. This act specifically targets all businesses that collect information for their use. The regulation protects the data within the private and personal sector, and, as a member of the EU, Germany has ratified its Act, Convention, and additional protocols with the EU according to the EU Data Protection Directive 95/46 (Wybitul 2017).

Cyber-Attacks

The nature of cyber-attacks in Germany are continuous and far-reaching. The German Federal Office for Information Security (BSI) reported that critical infrastructure in Germany is increasingly targeted in cyber-attacks (2018). According to the report, the BSI was alerted to 145 such incidents between July 1, 2017 and May 31, 2018. Most of the attacks were concentrated in the information technology (IT) and telecommunications sectors, followed by the energy industry. The BSI also estimated that the number of malware programs increased from 600 million to 800 million during the same period. The report highlighted that government networks were also in the sights of cyber criminals on a daily basis. The incidents included targeted campaigns as well as mass attacks, mostly through e-mails containing malware. Between July 2017 and May 2018, 28,000 threatening emails per month were caught in security filters on average before they could reach the intended inbox.

Because of this growing number of attacks, greater complexity of digital infrastructure and a larger volume of online data, the BSI stated that the likelihood of successful cybercrime had also increased. To illustrate the severity of cyberattacks in Germany, one can reference the hacking of the Bundestag or German Parliament. In May 2015, hackers managed to gain access to the Bundestag's internal server, launching an unprecedented attack by using "Trojan viruses." A representative of the German Parliament confirmed that data was stolen during the attack. This event prompted politicians to express their concerns about the Interior Ministry's ability to establish functioning cyber defense (The Guardian 2015).

In relation to this attack, more recently the data stolen during the Bundestag hacking was published online. The hacking leaked sensitive data belonging to hundreds of German politicians, celebrities and public figures and were published online via a Twitter account. The

cache of documents included personal phone numbers, addresses, internal party documents, credit card details and private chats. The hacking affected all of the main German political parties except the far-right Alternative for Germany (AfD) (The Guardian 2019).

The examination of cyber-attacks in Germany shows that the political and social ramifications of cybercrime are not always immediately apparent. While Germany thought they had effectively responded to the attack, recent developments have proven otherwise.

Examining the Policy Response

The BDSG was amended in 2009 and 2010 with three amendments: Novelle I was a new regulation of the activities of credit bureaus and their counterparties (especially credit institutions). The content of Novelle II included changes to the privileges for trading, new regulations for market and opinion research, opt-in coupling ban, employee data protection, order data processing, new powers for the supervisory authorities and new or expanded fines, information obligations in the event of data breaches and dismissal of protection for data protection officers (DPO). Novelle III was a small sub-item within the law that implemented the EU Consumer Credit Directive (Wyitbul 2017).

In 2018, Germany saw not only the introduction of GDPR but the new German Privacy Act (BDSG-new) as well. The BDSG-new complements, specifies and modifies the GDPR. It provides rules for specific topics, e.g. for data processing in the context of employment, the designation of a data protection officer, scoring and credit checks as well as profiling (Wyitbul 2017). In this context, it is evident that the restrictive reforms made in German policy were prompted by the introduction of GDPR. The GDPR was introduced to minimize security breaches, data protection issues and other instances of cybercrime. The evolution of German digital policy shows how the consecutive and restrictive policies implemented post-cyber-attacks can be interpreted as a reaction to the cybersecurity issues being faced at the time.

Methodology

In order to test my hypothesis that the number of cyber-attacks affects digital trade restrictiveness scores, I collected data from the 2018 DTRI and the 2018 ENISA report and conducted a simple linear regression. The idea of a digital economy is relatively new, and it was not until recently that these variations became problematic. We know that participation in the digital economy and digital trade has positive effects on a nation's economy, but what remains unclear is what factors influence a country's open or restrictive approach to digital trade strategy. The information collected for this analysis was obtained from two databases that used figures from the year 2018. By analyzing the variations in the national digital strategies described in the divergences section, I am able to conclude that these variations are present even among similar countries. Furthermore, I am able to take this information observed from the divergences and compare it with the Digital Trade Restrictiveness Index (DTRI) score in order to determine if their score is consistent with their national strategy. The DTRI also provides me with the ability to compare this score with that of other countries so that I can assign "high" and "low" scores for reference. This paper will aim to answer the research question by examining one independent variable that I believe has a profound effect on a country's DTRI score. For example, do countries with high rates of cyber-attacks have higher DTRI scores? More specifically, does an increased number of cyber-attacks on a country contribute to a more restrictive strategy in terms of digital trade? This is done by performing a bivariate regression analysis using Microsoft

Excel. A bivariate regression analysis involves analyzing two variables to determine the strength of the relationship between them. My goal is to determine whether or not the independent variable (number of cyber-attacks) impacts a country's Digital Trade Restrictiveness score (dependent variable) and to establish a relationship between cyber-attacks and variations among Member States.

Empirically, I am expecting to see that countries with increased instances of cyber-attacks will have higher DTRI scores. I hypothesize this because I expect that countries who are frequently targets of cyber-attacks are more aware of their vulnerability than other countries that are not frequent targets. Therefore, the target countries respond and react by implementing restrictive measures in order to minimize their potential to fall victim to more cybercrimes. The implementation of these restrictive measures is indicative of a higher DTRI score.

As previously mentioned, the independent or predictor variable is the number of cyber-attacks experienced by a specific country. This figure was originally expressed as a percentage because it represents the percentage of the country's entire population. I converted this unit into a decimal for the purpose of expressing both variables in the same unit of analysis. This variable measures the amount of cyber-attacks in each of the 28 EU Member States (See Figure 2). The figures used for the total populations of each EU Member state were obtained from The United Nations Population Division Database from 2018. The data for the independent variable, the number of cyber-attacks experienced in each Member state, was collected from the 2018 ENISA report.

The figures for the dependent variable, the DTRI score, were obtained from the 2018 DTRO Report. (See Figure 3.) The DTRI measures how countries in the world restrict digital trade. The dependent variable was measured using the DTRI score because the variations being analyzed include an individual country's openness to digital trade or digital topics relative to another country/countries. The DTRI score is expressed as a decimal because the scores can vary between 0 (completely open) and 1 (virtually closed). The average score of the EU-28 is .37 meaning the average EU country is more open than closed. The DTRI is based on a wide spectrum of digital trade policies covering more than 100 policy measures across 64 countries worldwide. The Index is the first global initiative to provide transparency of applied digital trade restrictions and sheds light on how countries compare with each other. The Index is based on the Digital Trade Estimates (DTE), a database developed by ECIPE.

Results

Model 1 examines the relationship that cyber-attacks have on a country's DTRI score by performing a linear regression analysis (See Figure 4). Before conducting this analysis, I expected to find that a country with increased cyber-attacks would have a DTRI score closer to 1 (virtually closed). Model 1 (See Table 1.) tells us there is a positive relationship between the number of cyber-attacks a country experiences and their respective digital trade restrictiveness. For each additional increase in the number of cyber-attacks, the overall DTRI score increased by 0.280. This tells us that when a country's DTRI score increases, their policies on digital trade become more restrictive. The r^2 was 0.113. This indicates that the model accounts for approximately 11% variance in the dependent variable. Unfortunately, this model was not found to be statistically significant, meaning that we fail to reject the null hypothesis. This could be a result of the two variables being endogenous to each other, in that one variable could determine the other. I conclude that this model is not a good fit for determining what explains the cross-

national variations in digital trade restrictiveness. I believe that this study would have been different had I included more variables.

Table 1. Effects on Digital Trade Restrictiveness Score

	Model 1
Cyber Attacks	0.280 (0.154)
Dependent Variable	0.324*** (0.029)
n	27
r^2	0.113

*= p<0.05; **=p<0.01; ***=p<0.001

Discussion of Findings/Conclusion

Based on the findings in the regression analysis, I can confirm that my original hypothesis was supported by observing that countries subject to more cyber-attacks have higher DTRI scores. The differences of the DTRI scores can explain the variations in national strategies towards digital trade. Although these findings were supportive of my hypothesis, the lack of statistical significance indicates that further research on this topic is required in order to determine a more complete cause for variations in strategy.

In this context, it should be acknowledged that there are other variables that serve as explanatory factors in addition to cyber-attacks. For instance, a country's levels of digital integration and cyber-readiness should be included as potential factors. Digital integration should be considered an explanatory factor because countries with lower digital integration are likely not as concerned with their digital strategies as countries who have higher digital integration. A country's cyber-readiness is determined by a multitude of factors such as, national strategies, defense and crisis response, incident response, diplomacy and trade, information sharing, E-crime and law enforcement and cyber R&D (France Cyber Readiness Assessment 2016). Cyber readiness could potentially assist in the explanations for strategy variations because countries who are more prepared are likely to be less vulnerable. (See Figure 5.) This theory is exemplified in the fact that countries with low technological readiness have seemingly high DTRI scores. For example, countries such as, Indonesia, India, Vietnam and Russia (DTRI 2018).

This study has presented a trend that northern countries have high DTRI scores. Therefore, another explanation that should be explored is a north-south divide. Although there may be merit in this argument, the north-south divide should be explored for divisive factors other than economic development. According to ECIPE, the DTRI is negatively associated with levels of economic development. The Index clearly shows that higher levels of digital trade restrictiveness are particularly observable in countries which are economically less developed (ECIPE 2018).

The aim of this study was to explain cross-national variations in digital trade restrictiveness. After reviewing the literature and studying specific cyber-attack events throughout Europe, it becomes clear that Member States are troubled as to why there is a negative connotation associated with the word "variation." The EU has consistently urged for the completion of the Digital Single Market indicating that they believe these variations are harmful rather than beneficial. This is based on the fact that the DSM seeks to harmonize digital trade rules and eliminate diverging national strategies. This analysis has led me to believe that the word "variation" in the context of the EU is almost always negative due to the rhetoric put forth by the EU institutions indicating that variations result in fragmentation. However, variations in national strategies towards digital trade and other digital aspects have given Member States the ability to address their own national concerns because, as history has shown, there is no "one size fits all" for every EU government sector.

The case studies presented in this paper have shown how cyber-attacks contain variation themselves in that the magnitude of attacks differs from country to country. Some Member States are frequent targets of cyber-attacks such as France and Germany. As previously mentioned, France and Germany have been identified as the most digitally restrictive countries in Europe and also have high numbers of cyber-attacks (ECIPE 2018). While countries like Denmark are similar to France and Germany in terms of the number of cyber-attacks experienced, they are not as digitally restrictive. This has provoked the thought that a Member state's relationship to the EU may affect their DTRI score.

France and Germany are considered to be super powers within the EU. They are two highly Europhilic countries, a fact which could potentially contribute to their DTRI score. By polarizing themselves in the sense that they have significantly more restrictive policies when compared to other Member States, the digital trade gap widens and creates doubt in the ability for national digital strategies to coexist within the EU. While the statement mentioned above is hypothetical, the relationship of a Member state to the EU and strategies towards digitalization require further exploration. In the process of conducting this analysis, the issue emerges as to whether the Digital Single Market Strategy is best for Europe. The variations that exist within the EU are what makes it a structure unlike any other complex political entity and trying to eliminate those variations potentially undermines the values of the EU. A suggestion for further research would be to explore alternative options to improve data sharing without compromising the values upon which Member States build their national strategies.

This paper has explored the explanations for variation in digital trade strategies and ultimately proposed a new variable to provide clarity on the issue. This paper presented the hypothesis that increased cyber-attacks result in higher DTRI scores and has tested this hypothesis through a combination of a qualitative and quantitative methods. The evolution of cyber-attacks in France and Germany, coupled with the timing of the policy reforms that occurred in order to respond to these attacks, prompted further testing of this hypothesis on the remaining EU-28. Through a simple linear regression, it was concluded that there is a relationship between the two variables of cyber-attacks and DTRI scores but not strong enough to be considered statistically significant. The results of the analysis encouraged a discussion suggesting further research in this area and offered potential variables that should be considered in future developments.

Appendix

Figure 1. Obtained from: E-Trade for all *Europe's Data Privacy Rules Set New Global Approach to Consumer Rights.*

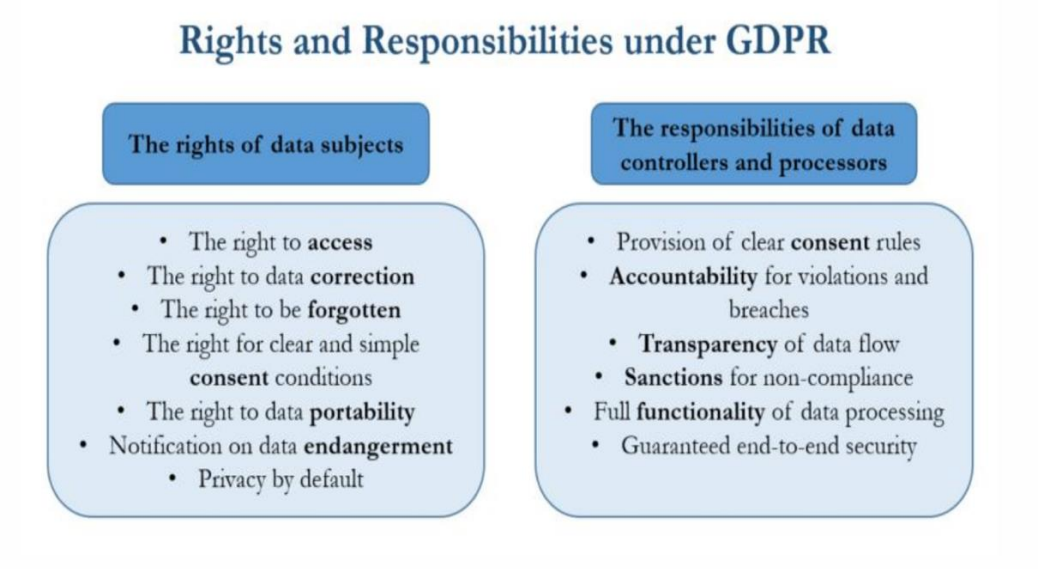


Figure 2. INDEPENDENT VARIABLE 1: CYBER ATTACKS
Data obtained from: *ENISA Report 2018*
The United Nations Population Division Database from 2018

EU Countries	Total Population	Population who has experienced cyber-attacks
Austria	8,766,201	.18
Belgium	11,562,784	.20
Bulgaria	6,988,739	.08
Croatia	4,140,148	.14
Cyprus	1,198,427	.14
Czech Republic	10,630,589	.17
Denmark	5,775,224	.24
Estonia	1,303,798	.17
Finland	5,561,389	.15
France	65,480,710	.29
Germany	82,438,639	.23
Greece	11,124,603	.11
Hungary	9,655,361	.14
Ireland	4,847,139	.17
Italy	59,216,525	.17
Latvia	1,911,108	.16
Lithuania	2,864,459	.13
Luxembourg	596,992	.20
Malta	433,245	.17
Netherlands	17,132,908	.27
Poland	38,028,278	.16
Portugal	10,254,666	.15
Romania	19,483,360	.18
Slovakia	5,450,987	.09
Slovenia	2,081,900	.13
Spain	46,441,049	.35
Sweden	10,053,135	.20
UK	66,959,016	.26

Color	**Meaning**
Green	Low
Yellow	Case Study Countries
Red	High

Figure 3. DEPENDENT VARIABLE: DIGITAL RESTRICTIVENESS
Data obtained from: *Digital Trade Restrictiveness Index 2018*
The United Nations Population Division Database from 2018

EU Countries	Total Population	Digital Restrictiveness
Austria	8,766,201	0.39
Belgium	11,562,784	0.39
Bulgaria	6,988,739	0.39
Croatia	4,140,148	0.36
Cyprus	1,198,427	0.36
Czech Republic	10,630,589	0.32
Denmark	5,775,224	0.46
Estonia	1,303,798	0.32
Finland	5,561,389	0.42
France	65,480,710	0.51
Germany	82,438,639	0.48
Greece	11,124,603	0.39
Hungary	9,655,361	0.32
Ireland	4,847,139	0.32
Italy	59,216,525	0.42
Latvia	1,911,108	0.32
Lithuania	2,864,459	0.36
Luxembourg	596,992	0.36
Malta	433,245	0.36
Netherlands	17,132,908	0.39
Poland	38,028,278	0.39
Portugal	10,254,666	0.32
Romania	19,483,360	0.35
Slovakia	5,450,987	0.32
Slovenia	2,081,900	0.36
Spain	46,441,049	0.32
Sweden	10,053,135	0.39
UK	66,959,016	0.38

Color	**Meaning**
Green	Low
Yellow	Case Study Countries
Red	High

Figure 4. Microsoft Excel *Regression Analysis*

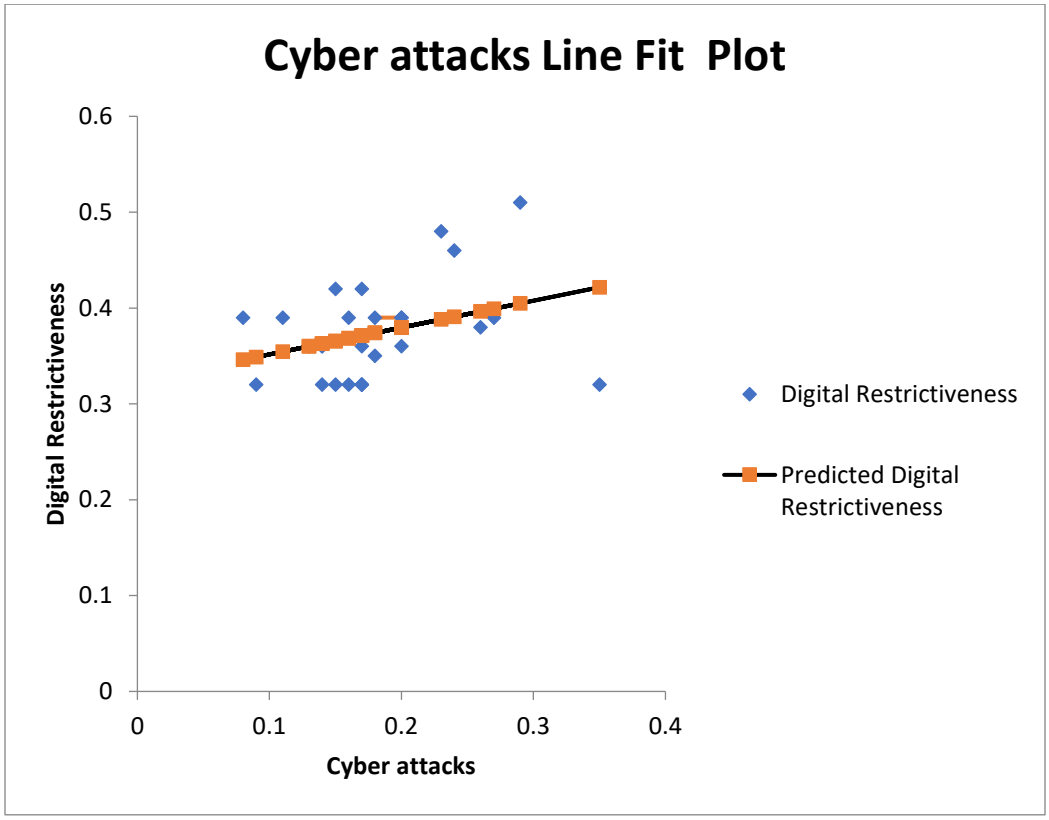
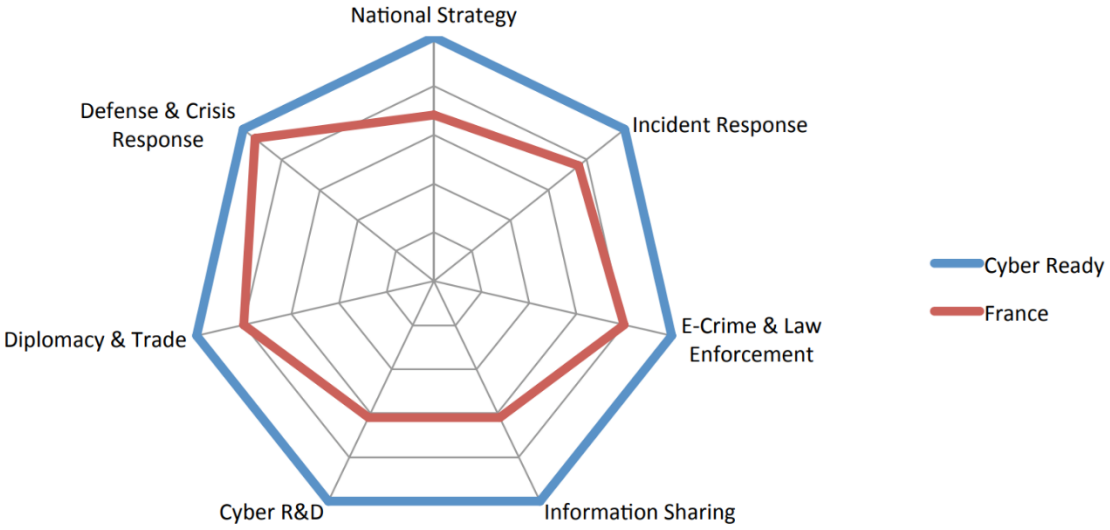


Figure 5. Obtained from: *France Cyber Readiness Assessment (2016)*



France Cyber Readiness Assessment (2016)

References

BBC News. 2011. *Cyber Attack on France Targeted Paris G20 Files.* BBC News. March 7. https://www.bbc.com/news/business-12662596.

BBC News. 2017. *France thwarts 24,000 cyber-attacks against defence targets.* BBC News. January 8. https://www.bbc.com/news/world-europe-38546415

Blond, J. L. 2019. *German Politicians' Personal Data Leaked Online*. The Guardian. Guardian News and Media. January 4. *https*://www.theguardian.com/world/2019/jan/04/german-politicians-personal-data-hacked-and-posted-online.

Business Europe. 2017. *Business Europe's views on Digital Trade [Position Paper].* Business Europe. https://www.businesseurope.eu/sites/buseur/files/media/position_papers/rex/2017-02-06_digital_trade.pdf

Corera, G. 2016. *How France's TV5 Was Almost Destroyed by 'Russian Hackers'*. BBC News. October 10. https://www.bbc.com/news/technology-37590375.

Cousiel. 2019. *Building a European Data Economy.* Digital Single Market - European Commission. January 24. https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

Deutscher Bundestag. 2016. *Privacy Policy.* German Bundestag. November 15. https://www.bundestag.de/en/service/privacy.

Digital Trade Restrictiveness Index. 2018. *DTRI Rankings.* ECIPE. Chapter 2. http://ecipe.org/wp-content/uploads/2018/04/Chapter-2.pdf

Dreyfus. 2018. *French Data Protection Act: What's New?* Dreyfus. December 4. http://www.dreyfus.fr/en/uncategorized-en/french-data-protection-act-whats-new/.

ECIPE. 2018. *ECIPE – European Centre for International Political Economy*. https://ecipe.org/publications/the-next-steps-for-the-digital-single-market-from-where-do-we-start/.

ECIPE. 2019. *Digital Trade Estimates Report.* ECIPE – European Centre for International Political Economy. https://ecipe.org/dte/dte-report/.

ENISA. 2019. *Exposure to Cyber-Attacks in the EU Remains High - New ENISA Threat Landscape Report Analyses the Latest Cyber Threats.* ENISA. January 30. https://www.enisa.europa.eu/news/enisa-news/exposure-to-cyber-attacks-in-the-eu-remains-high.

Esteana. 2019. "Shaping the Digital Single Market." Digital Single Market - European Commission. February 15. https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

ETrade for All. 2018. *Europe's Data Privacy Rules Set New Global Approach to Consumer Rights.* ETrade for All. May 31. https://etradeforall.org/europes-data-privacy-rules-set-new-global-approach-to-consumer-rights/.

EU Trade Commission, and C. Malmström. 2015. *Trade for All - Towards a More Responsible Trade and Investment Policy.* European Commission. http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf.

European Commission. 2016. *Directive 95/46/EC. European Innovation Partnership* - European Commission. August 26. https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en.
European Commission. 2018. *Data Protection.* European Commission. November 14. https://ec.europa.eu/info/law/law-topic/data-protection_en.
European Commission. 2018. *Digital Economy and Society Index.* European Commission. http://news.ucamere.net/StudyInternationalDigitalEconomyandSocietyIndex2018.pdf
European Commission. 2019. *Tallinn Digital Summit – Factsheets.* European Commission. https://ec.europa.eu/commission/publications/tallinn-digital-summit-factsheets_en.
Federal Office for Information Security. 2019. *Bundesamt für Sicherheit in der Informationstechnik.* BSI. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.html.
Hathaway, M. 2016. *France Cyber Readiness at a Glance.* Cyber Readiness Index 2.0. Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/CRI/CRI_France_Profile_PIPS.pdf
Information Technology and Innovation Foundation (ITIF). 2017. *Information Technology and Innovation Report: Cloud Computing is Transforming Modern Manufacturing.* MH&L U.S. Roadmap. June 27. http://www.mhlroadmap.org/information-technology-innovation-foundation-report-cloud-computing-transforming-modern-manufacturing/
Negreiro, M. 2015. *Bridging the Digital Divide in the EU.* European Parliamentary Research Service. European Parliament. December 2015. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/573884/EPRS_BRI(2015)573884_EN.pdf.
Ogee, A. 2015. *The 2015 Report on National and International Cyber Security Exercises.* European Union Agency for Network and Information Security (ENISA). December 2015.
Perritt, Henry H. Jr. (1998) *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance.* Indiana Journal of Global Legal Studies: Vol. 5: Iss. 2, Article 4.
Proust, O. and Goossens, G. 2016. *Privacy, Security and Information Law*. Privacy and Information Law. https://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law.
Pusterla, E. R. G. 2018. *Credibility of Sovereignty - the Political Fiction of a Concept*. Place of publication not identified: Springer International PU.
Reding, V. 2015. *Digital Sovereignty: Europe at a Crossroads.* European Investment Bank Institute. October 26. http://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf
Rogowski, R. 1989. *Commerce and Coalitions: How Trade Affects Domestic Political Alignments.* Journal of Economic History. Vol. 50: Iss. 2, 509-510.
The Guardian. 2015. *Pro-Russia Group Claims Cyber-Attack on German Government Websites.* The Guardian. Guardian News and Media. January 7.

https://www.theguardian.com/world/2015/jan/07/pro-russian-group-cyber-attack-german-government-websites-angela-merkel-ukraine-prime-minister.
United Nations. 2019. *Population.* United Nations. https://www.un.org/en/sections/issues-depth/population/.
University of Manchester. 2019. *Trade Wars Are Growing – and Developing Countries Are Shaping the Agenda*. University of Manchester. March 15. https://www.manchester.ac.uk/discover/news/trade-wars-are-growing/.
Willsher, K. 2017. *Emmanuel Macron's Campaign Hacked on Eve of French Election.* The Guardian. Guardian News and Media. May 6. https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election.
Wong, P. 2002. *ICT production and diffusion in Asia Digital dividends or digital divide?* Information Economics and Policy. Vo. 14: Iss. 2, 167-187.
World Economic Forum. 2019. *Shaping the Future of International Trade and Investment System Initiative*. World Economic Forum. https://www.weforum.org/projects/digital-trade-policy.
Wriston, Walter B. 1997. *The Twilight of Sovereignty*. Bridgewater, NJ: Replica Books.
Wybitul, T. 2017. *Germany Publishes English Version of Its National GDPR Implementation Act.* 2017. HL Chronicle of Data Protection. August 24. https://www.hldataprotection.com/2017/08/articles/international-eu-privacy/germany-publishes-english-version-of-its-national-gdpr-implementation-act/.

.