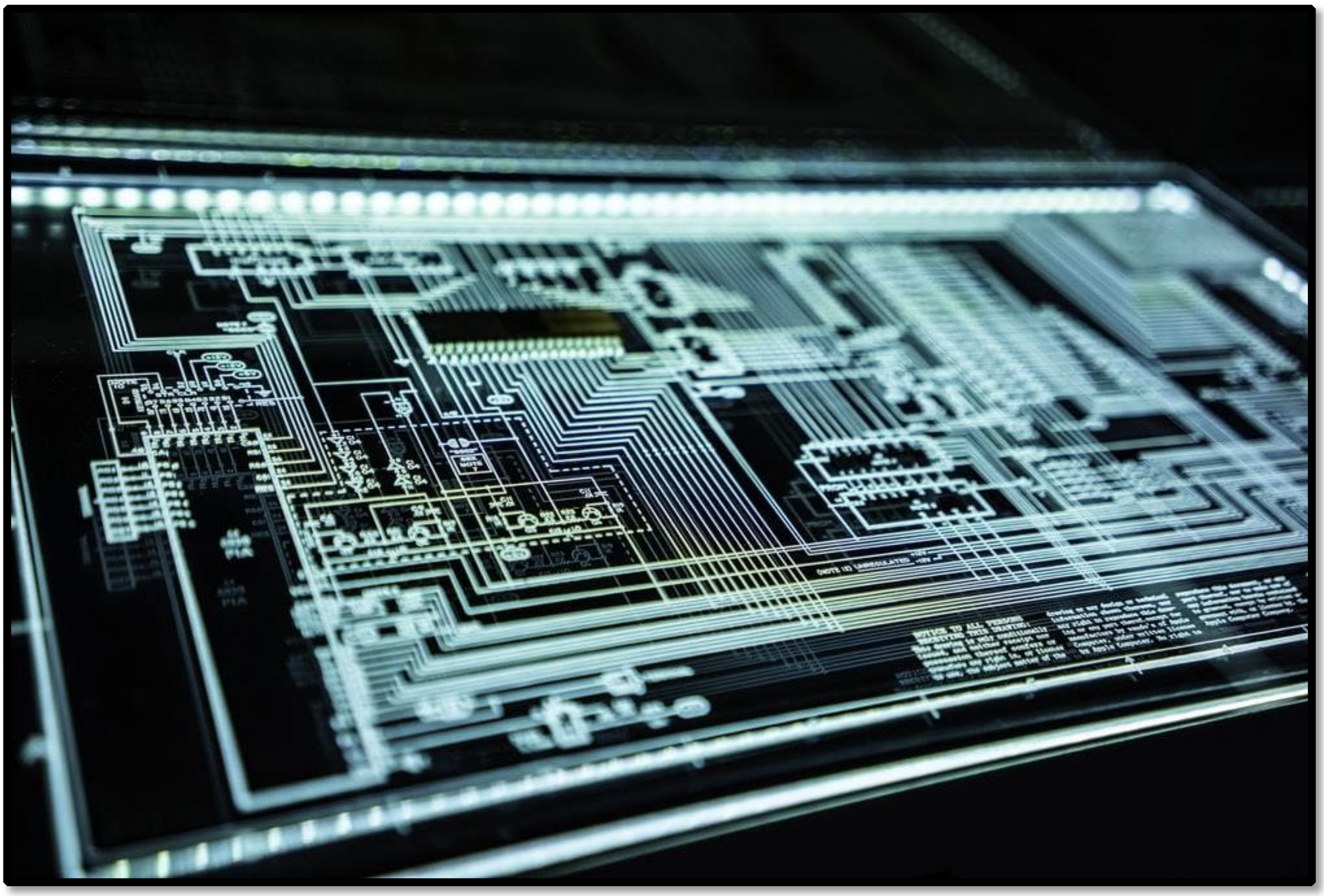


Southern University of Denmark

The Faculty of Business and Social Sciences

1/6/2022

International security and law

Master Thesis:

Weaponized interdependence, cyber resilience, and financial institutions

Frederik Hurwitz, 12/07/1995, Exam nr.: 489179

André Ken Jakobsson

Number of strokes: 161.723

Table of content

1. Introduction

The liberal international order has dominated western ideology and society since the 1940s, however, a shift in attitude and actions from states such as Russia and China have highlighted how these rule-based, structured relationships might not be as successful as we thought previously. Since the end of World War 2 democratic liberal western countries have followed the idea of open markets, security cooperation, monetary cooperation, and promotion of liberal democracy that could create a stable and peaceful world. States such as China and Russia, which do not believe in the same democratic values, showcase through their actions that they do not adhere to the same international standards as states of liberal ideology. From a realist perspective, actors with ill intentions and powerseeking behavior would not find it suitable to follow ideas of interstate cooperation and peaceful interdependence. States that are purposely going against the liberal order, work to promote ideas that undermine the nature of interdependence and liberal thought. In the end, it could put an end to the idea of interdependence and peace through mutual dependencies. Moreover, with the establishment of interdependencies throughout the last 40 years it has connected us even more, but scholars such as Farrell and Newman question whether this intention might have set the bad actors in a better position as we become dependent on their resources, whether, it be financial, energy or financial. Especially critical infrastructure such as energy, internet, information, monetary, and finance all depend on each other. However, one thing that has evolved that is affecting all entities is the security of our cyberinfrastructure. If it is not secure enough it could allow states with bad intentions to take advantage of cyber dependencies and network centralizations through coercive or direct actions. One example of European dependency on foreign projects is the talked about Nord Stream 2. Currently a very discussed topic in international and national politics across Europe and the United States. It has highlighted how Europe is and could even be more dependent on Russian gas in the future. It would allow Russia to weaponize our dependency on their gas and this might only be the beginning of influence from foreign and adverse states that seek to undermine European security. Moreover, there are other examples of Chinese projects that could serve to create a dependency on their goods or technology, facilitating what Henry Farrell and Abraham L. Newman call the “panopticon” and “chokepoint” effects. For Europe in general this is not an ideal situation, and a main part of this academic paper is to look at how the European Union is using regulations to combat these adverse events through cyber resilience.

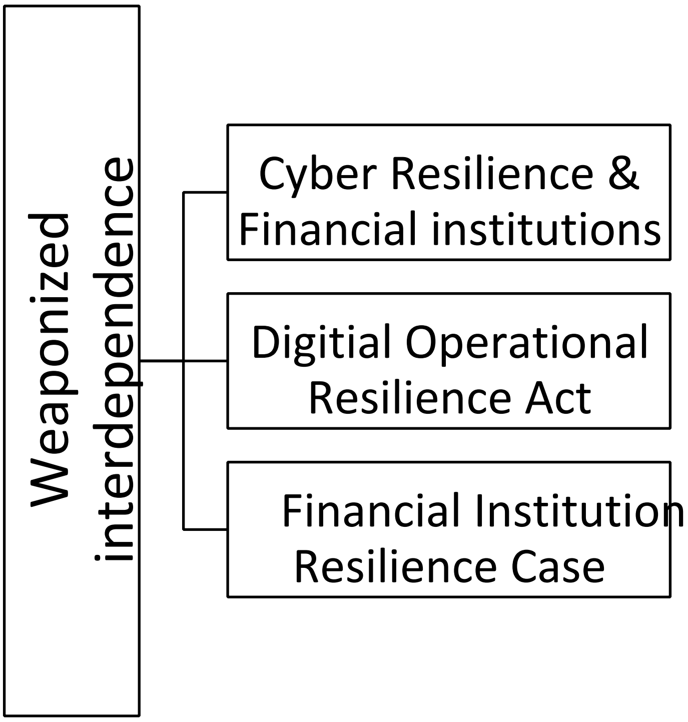
Furthermore, the globalized and interdependent world that is connected through the invention of the internet of things (IoT), has for years been the basic feature of a free and liberal world order and according to scholars such as Farrell and Newman interdependence is being weaponized by states and non-state actors to take advantage of the mutual dependencies that are the foundation of the liberal global order (Farrell & Newman, 2019). At the bottom of these dependencies, there is a world that is more connected than ever and that is a product of the global liberal order. With the emergence of the Internet of Things (IoT) our lives have become ever more connected than thought possible. It has affected all sectors of our daily lives, from the financial sector to how we communicate with each other. The interconnectedness of the internet and cyber in general is showing signs of producing both positive and negative impacts on society and the international order. Globalization and interdependency produce dependencies on central actors that allow them to gain such a substantial amount of power, that they can force other states with power solely based on interdependencies. Taking advantage of interdependencies is not a new phenomenon, the United States has been using its position as a global hegemon for decades. And studies have shown that in trade and banking the United States and the United Kingdom are exceptionally connected allowing them to generate a great amount of power in the global financial world through economic networks (Farrell & Newman, 2019). Furthermore, in a world connected through global online economic networks these premises allow states with a high level of interconnectedness and power over infrastructure to use these dependencies as a weapon against other states. One of the key factors that academics and international security actors look at is the level of centralized nodes in the online sphere. These nodes or "hubs" are large-scale networks that are seen as connection points in online infrastructure. Different nodes are more connected than others and those that show an overly complex system that produces asymmetric network structures. Those nodes are central to understanding how the online sphere can demonstrate and showcase how power and dependencies structures are highly interconnected and that some nodes are controlled by outside powers in Europe (Farrell & Newman, 2019). In Europe regulators and state, actors are starting to figure out and fight back as they fear states like the United States, China, or Russia are taking advantage of these dependencies. European resilience, i.e., the "ability to absorb change and disturbance and still maintain the same relationships"(C S Holling, 1973) is starting to gain more and more foothold as a response to weaponized interdependence. A reaction to the growing challenges facing Europe dependencies and peace is the Digital Operational Resilience Act or DORA.

This academic paper's overarching thesis is **how weaponized interdependence challenges European cyber resilience in financial institutions.** The paper will start at the top by analyzing how weaponized interdependence challenges financial institutions and how it is affecting their security. Moreover, the first part of the analysis will go into detail about how to obtain and enhance cyber resilience. The analysis is done by using Benoît Dupont's five dimensions of cyber resilience. Thereafter, it will use a social constructivist perspective of weaponized interdependence, cyber resilience, and DORA. Lastly, an interview of the chief information security officer at The bank gives primarily cyber resilience, DORA, and security for financial institutions a real-life perspective and helps to support the thesis. The academic paper lays out the main thesis statement as the liberal and globalized world order is challenged by weaponized interdependence which puts pressure on financial institutions' cyber resilience because of the "panopticons" and "chokepoint" effects. Moreover, a social constructivist perspective of European cyber resilience will support better analysis of European cyber resilience by providing a distinct way of understanding social and international reality and, by focusing on the role of ideas, identity, and norms in shaping state preferences and world politics.

Ontological security issues will also be used in the analysis regarding the social constructivist perspective of cyber resilience. Ontological issues are valuable in an interdependent international liberal order in Europe to understand how the future is going to be shaped. Generally, the project aims to answer what weaponized interdependence is and if it could be a security issue for European peace and security. What effect has the shift towards private actors had on the international order? The project will use the notion of how nodes or central "hubs" are producing asymmetric network structures and dependencies on foreign actors in cyberspace. The paper will examine the question of why are the European Union is creating a resilience act in cyberspace? What is the European Union pushing back against? This will be looked at in a case study of The bank Bank and its security issues when dealing with DORA. The projects will take it theoretical standpoint on weaponized interdependence and an ontological security understanding. When analyzing and discussing the case study the paper will deploy Robert K. Yins Case Study Method on The bank and DORA. Key concepts such as cyber resilience, financial institutions, and cyberspace will give the reader a general introduction to the field and allow the reader to gain the necessary knowledge to fully understand the challenges and issues facing cyber resilience in Europe.

2. Framework

Establishing a framework for this academic paper is valuable in understanding the underlying theoretic ideas and concepts that support the analysis and conclusion. To identify which key concepts are important for the academic report an easy-to-understand model is made to allow the reader to see how the different concepts are connected. After the framework, the relevant concepts and how the theory fits into the larger picture are outlined. Weaponized interdependence, DORA, and the The bank Bank interview is the overarching concept and case that the academic paper will take from its standpoint. Together with cyber resilience, ontological security, and financial institutions, it is the basis of understanding the context and theoretic outlook of the academic paper. In the analysis to introduce and analyze the challenges that face cyber resilience the starting point will be Dupont's five dimensions of cyber resilience. Furthermore, the reader needs to be given a historic context to both weaponized interdependences, cyber, and resilience, or else the academic paper could fail in giving the reader the right insight into the issues and challenges.


Weaponized interdependence
Cyber Resilience & Financial institutions
Digitial Operational Resilience Act
Financial Institution Resilience Case

2.1 Weaponized interdependence

In recent years, the concept of weaponized interdependence has gained traction in international relations. This refers to the use of economic, political, or military pressure to force another state or organization to comply with one's demands. "Weaponized interdependence" explains how the broad structural features of the global economy enable some states while constraining others, providing a theory of power in the new world order. The theory behind weaponized interdependence that this academic paper takes its standpoint in, is first of all the article “Weaponized Interdependence: How Global Economic Networks Shape State Coercion” by Farrell and Newman but also their book on the subject “The Uses and Abuses of Weaponized Interdependence”. Here they describe and explain their take on the emerging new theory that influences international security. Meanwhile, they explain that they are preventing destabilization mistakes by mapping the landscape of the new emerging world. The authors argue that this allows the academic and policy community to discuss and think about secondary sanctions and other forms of economic coercion as part of an emerging system, rather than discrete actions. One notable example of weaponized interdependence was Russia's use of energy exports to pressure Ukraine into submission in 2014. By threatening to cut off Ukraine's supply of natural gas, Russia was able to get Ukraine to agree to several sessions including a pro-Russian government and military base in Crimea. While weaponized interdependence can be an effective tool, it also carries with it an elevated risk of escalation. If not used carefully, it can easily lead to a full-blown conflict. Also, if a state is taking too much advantage of other dependencies, it risks those states and others bluffing and cutting the dependency altogether (Farrell & Newman, 2019, 2021a).

The figure above is a representation of the framework of the thesis. Outlining weaponized interdependence is a key concept in this academic research paper. The geostrategic outcome that comes from having control and power over the sphere of energy, financial goods, and information markets are increasingly going up. On the other side, so is the number of states that are in control of them. Resulting in countries controlling big portions of for example oil or energy. Weaponized interdependence is both used in conflicts as a direct means but can also be utilized as a coercive tool in conflicts. As seen when Russia invaded Ukraine and the answer from western states was to sanction and impose restrictions on financial, energy, and information markets. Essentially using the fact that Russia itself also is reliant and dependent on international goods (Foreign, 2022; Minami Funakoshi, 2022; Roth, 2022). The sanction on Russia is just one example of how the US or the West is using their global economic networks to achieve strategic and in this case military aims.

Globalization has according to Rosa Brooks's book on globalization created a world in which everything became e war. While states have become more dependent on each other for in some cases for good it has also meant that flows of finance, information, and physical goods across borders introduce both new risks for states and new tools to alternatively exploit or relieve those risks by both friends and foes (Brook, 2016). In Thomas Wright's book "All measures short of war" he describes the results as a world where unprecedented levels of interdependence are combined with continued competition for power. States in the international system are unwilling to engage in direct conflict but may still employ all measures short of war (Thomas Wright 2020).

Global Economic Networks are at the center of weaponized interdependence, and because of increased interdependence between states the threat picture is increasing, and this results in security concerns between states. With the emergence and development of the internet and financial communications, they are at the hearth of globalization and power. When globalization and interdependence first began being noticed by liberal thinkers the standard liberal account of interdependence paid attention to power but emphasized bilateral relationships. In today's world, we see that changes have occurred to this pattern and that global networks obscure fundamental patterns of mutual dependence. Larger states like the United States can exercise power to achieve strategic objectives in the international arena. Weaponized interdependence argues and makes a different assumption that those imbalances among states create the foundation for weaponized interdependence. Farrell And Newman argue that the imbalance is based upon network topography that generates enduring power imbalances between states. This means that more powerful states are more likely to sit on top of those network topographies and control them. Weaponized interdependence draws upon sociological and computational research on large-scale networks. They demonstrate the tendency of complex systems to produce asymmetric network structures. The network is structured as two basic elements: nodes or "hubs", which represent the actors or locations within the network. These structures can produce far more asymmetric networks than thought before and the ties, which connect these nodes. Because some hubs are far more connected than other states that are in control of said hubs and can utilize their power over other states, this is exactly where weaponizing interdependence comes into play (Farrell & Newman, 2019). States can leverage a set of powers over others through their relations with states, just as mentioned in the example given about Russia and Ukraine. Other examples of purely weaponized interdependence by one state can also be seen in cases such as the relationship between the US and Iran (Hafezi, 2021; Motamedi, 2022). The big issue with global economic networks at this moment in time is that they are not the kind of openended networks that are capable of overturning power asymmetries and topping political hierarchy. On the other hand, global economic networks tend to be highly centralized (Farrell & Newman, 2019). For example, the dollar clearing system, which is crucial to international financial flows, runs through a very small number of key United States institutions. The nodes, in turn, can become paths for coercive or direct state control. Having jurisdiction over the key nodes in an important global network along with appropriate institutions can leverage a state's power substantially. Thus, it means it can weaponize the network, using it to conduct surveillance or to block others from accessing the network in question (Farrell & Newman, 2021a; Oatley, 2021).

The history between Iran and the United States is a good example of how a global actor and more powerful state can leverage its power over another state through weaponizing interdependencies. The history between the United States and Iran is a long and complicated story, however, to quickly summarize it is a "bitter" rivalry between states. Through the years there have been sanctions that started during the Carter presidency with the "Iran Hostage Crisis" (Hewitt & Nephew, 2019), thereafter, it was during the Reagan presidency he imposed an arms embargo on both Iran and Iraq because Iran's actions from 81´ to 87 against the US and other vessels in the Persian Gulf (Levs, 2012). Then it was Clinton that imposed what some label as some of the toughest sanctions on Iran in 1995, the main reason was because of the Iranian nuclear program and Iranian support for Hezbollah. The US prohibited all US trade he Iran's oil industry (Katzman, 2022). After that came the Bush presidency which also imposed sanctions through the U.S Department of the Treasury ruled against editing or publishing scientific manuscripts from Iran and stated that U. S. scientists could not collaborate with Iranian scientists (Brumfiel, 2004). Furthermore, then Obama came into power, and he signed into law the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 CISADA, which greatly enhanced restrictions on Iran, including the rescission of the authorization for Iranian-origin imports for articles such as rugs, pistachios, and caviar (Ferrari, 2010). Further sanctions were also created; however, the picture is starting to clear on how the United States uses its power over Iran through sanctions and interdependencies. Also during the Trump era, further sanctions were created, during this time the U.S Treasury Department investigated possible violations against the U.S sanctions by China's state-controlled technology company Huawei (Stecklow, 2020; Woo & Viswanatha, 2018). The effects of all the sanctions are there, however, after so many years it has not stopped, what the U.S tried to do in the first place, to stop terrorist funding. And one could argue that this relationship has shaped the middle east for the last 40 decades. However, it exemplifies what weaponized interdependencies can be used for, but also the example has roots in westernization and globalization that in the 1950s and 1960s, were a goal for the United States in the middle east. This is a long story to go into but the US and the UK reinstated the western orientated Shah in 1953 (Risien, 2000), however, for years the population was not happy with westernization of the country and in 1979 the Iranian revolution took over.

Furthermore, all the sanctions towards Iran have led Europe to establish the instrument in support of trade exchanges. INSTEX is a European special-purpose vehicle established on 31 January 2019. Its mission is to facilitate non-USD and non-SWIFT transactions with Iran to avoid breaking U.S. sanctions. At time of implementation the ‚SPV was limited to humanitarian purposes only (Girardi, 2019; Irish & Alkousaa, 2019).

Furthermore, political control or authority over the central hubs is highly powerful as they give the state power over information. This information is seen in international central network structures in the form of money, goods, and financial information. Gaining control over international central nodes allows states to utilize this information and possibly it to their advantage. States can exploit vulnerabilities in energy storage or stop information flows only to push and control their adversary. The chokepoints create an effect where more powerful states can weaponize their dependence on said hubs. Farrell and Newman lay out two strategies that allow states to gain power advantages. First, advantaged states use their network position to gain information advantages via their network control. Lastly, states use the network advantage to cut off adversaries from the network entirely (Farrell & Newman, 2019). Weaponized interdependence is the first concept to understand as the academic paper begins analyzing and discussing why Europe is focusing on cyber resilience.

Other liberal scholars claim that globalization creates decentralized networks that generate new opportunities for cooperative diplomacy. The guiding idea for these thinkers is that globalization is best understood as a nonhierarchical network in which new arts of cooperation consist in identifying the right relationships. The relationship is picked among a variety of possibilities that serve to achieve the job for a given state. In that sense, power is with others rather than over others. However, in this academic paper, the notion of interdependence is aligned with Farrell and Newman’s account and argument. Their approach takes the stance just like the liberal account that networks are serious, and they affect states’ power. However, it starts from a different premise. First, they argue that networks are of sociological sense and nature, meaning that they shape what actors can and cannot do. Secondly, network structures can have important consequences on the distribution of power. They do not result in a flat world of diffuse power relations, on the other hand, they result in a specific, tangible, and persistent arrangement of power imbalance. Henry and Farrell specifically argue that “key global economic networks like many other complex phenomena tend to generate ever more asymmetric topologies in which exchange becomes centralized, flowing through a few specific intermediaries” (Farrell & Newman, 2021a).

To fully understand weaponized interdependence, it is important to know what the two forms of power that can be exercised are. Farrell and Newman lay out those two as “the panopticon effect” and “the chokepoint effect”. The first effect of the panopticon is a borrowed metaphor from Foucault in his metaphor it is all about building a circular prison. Which is controlled from the middle by a single entity. In weaponized interdependence, it is the central nodes of a network that can see all of the communications or generally all of the flows of information coming through that network. And that gives the one in control an extraordinary amount of power over others in that network or “node”. Practically it gives the person in the “middle” a very high degree of vision into what is happening elsewhere in the world. Perhaps that node gives information on how potential adversaries are communicating with each other. In financial institutions, it might be how they are sending money to each other. This gives the one in control a substantial amount of strategic power in being able to anticipate what other actors are doing. It could also be possible to work against your allies or adversaries or work to shape their activities in ways that advantage you as the controller of the panopticon. Furthermore, the second effect in this is the “chokepoint effect” whereas panopticons were about surveillance this is an effect of having a sufficient amount of control over a central node. Therefore, it allows you to block access to that network, and basically, you can block certain actors off the network. Then the one in control might be effectively denying an actor access to the network as a whole. A good example of this is how the EU, the US, and their allies agreed to cut off several Russian banks from the main international payment system known as Swift (Prescott, 2022).
(Farrell & Newman, 2019)

2.2 Cyber resilience and financial institutions

In the face of adverse cyber events that give the possibility of disastrous consequences, cyber resilience is the ability to positively adapt before it occurs. Preparing, responding, and recovering from cyberattacks and data breaches is of great importance for international actors and importantly states across the world. If a state is not cyber resilient i.e., cannot defend against cyber threats, have adequate cybersecurity risk management, and can guarantee business continuity during and after cyber incidents it can have major consequences. And cyber resilience is seen as an evolution in cybersecurity thought and understanding, that allows states to withstand attacks. Cyber resilience is on its basis development of the mindset and represents a shift from protection and avoidance of adverse cyber events to the development of a fail-safe system to anticipate and plan for undesirable cyber events. The definition of cyber resilience is “the ability to continuously deliver the intended outcome despite adverse cyber events” (Björck, Henkel, Stirna, & Zdravkovic, 2015). Thus, in the context of cyberspace, it is the ability to prepare, absorb, recover, and adapt to the effects of adverse cyber-attacks. Gaurav Banga CEO and Ph.D. student in computer science describe cyber resilience as “our ability to succeed in the face of adversity” (Banga, 2020). Davis echoes his description by describing it as “the ability of a system to return to its original or desired, state after being disturbed” (Davis, 2015). For example, a financial institution is resilient if it takes action to adapt and survive because of that in the face of an adverse event. A good description of it but how does it apply to cyber security? The most common approach to defining cyber resilience and how it applies to cyber security is to take a 360-degree view of cyber security. A perspective that includes prevention, detection, response, and recovery. The connection between cyber security and cyber resilience is vital and to align an organization's cyber attitude to reach beyond just cyber security and into the aspect of business continuity, it is important to further understand the role that cyber resilience employ and what cyber security is. For example, a Ponemon-Sullivan report, sponsored by Resilient an IBM-backed company, defines cyber resilience as the “alignment of prevention, detection, and response capabilities to manage, mitigate, and move on from cyber-attacks.” (Ponemon-Sullivan, 2015).

Furthermore, allowing a state to deliver a much-needed mechanism that could be taken out during cyber-attacks. As a key concept of cybersecurity studies, there is a proven link between cyber security and the importance of cyber resilience when protecting government and essential non-government systems One of the main advantages of cyber resilience is that it enables a complex organization to prepare for adverse events and keep operating under very challenging circumstances. This article seeks to explore the challenges and issues corresponding to cyber resilience and financial institutions. However, the notion of cyber resilience can be applied to all kinds of critical infrastructure (Dupont, 2019; Irene Christine & Thinyane, 2020). Moreover, an important notion that Davidson et al. argue and conclude in their academic paper on resilience thinking is that for delivering the much-needed mechanism for resilience, thinking must be open to alternative traditions and interpretations if it is to become a theoretically and operationally powerful paradigm. Thus, this is the same case for cyber security and financial institutions, this is a key aspect (Davidson et al., 2016).

The reason why cyber resilience is so important today is the evolution of cyber-attacks and the effects on both technical systems and socio aspects. In the modern world, where social connection is greatly facilitated by centralized technical systems it is to be understood as an arrangement of social and technical systems. The social dimension of cyber resilience comprises the social, cultural, political, and economic circumstances. Normal protection of vital cyber infrastructure is not enough anymore, and it cannot adequately secure vital information, data, and network security. States and the European Union are not in favor of having a risk of adverse cyber events taking out key infrastructure, it can impact confidentiality, integrity, and availability of financial institutions every day. Therefore, are the European Union looking to great greater security for its institutions through cyber resilience acts that great a fundament for a baseline for security in those institutions. Furthermore, several benefits of cyber resilience that make it an advantage for states and institutions are the ability to reduce financial loss, enhance security systems and enhance security reputations (Irene Christine & Thinyane, 2020). And first of all, cyber resilience links directly to weaponized independence and the way states are taking advantage of key network hubs. If enemy states can cut off central information lines such as internet connectivity it can directly hurt financial institutions just as in the case of Huawei in European countries (Irene Christine & Thinyane, 2020). Cyber resilience is further linked to DORA which will be connected to it in the next section. But the reader needs to understand how weaponized interdependence and cyber resilience directly tie into each other.

Financial institutions and cyber resilience are two main aspects of cyber-attacks today. A financial institution to summarize it for the reader is labeled by Investopedia.com as a company engaged in the business of dealing with financial and monetary transactions. They encompass a broad range of business operations within the financial service industry, and they can include banks, trust companies, insurance companies, brokerage firms, and investment dealers. In this academic paper and the case later described the focus is on banks and the impact weaponized interdependence and cyber resilience have on them (Hayes, 2022). With the growing number of cyber-attacks that aim at financial institutions and the impossibility of protecting the integrity of critical computer systems, cyber resilience in financial institutions is important for the function of society. Cyber resilience in this context offers a desirable complementary option to the existing paradigm of cybersecurity (Dupont, 2019).

The important questions now are why do weaponized interdependence, cyber resilience, and financial institutions matter for states or other organizations? First, no organization is safe in the growing sphere of cyberspace. An example that illustrates how sophisticated cyberattacks today and how fragile cyber security systems are even for organizations with the highest level of security is the Israeli Spy Case. The New York Times and the Washington Post brought a story in their newspaper in 2017 detailing how Israeli spies had infiltrated the systems of the cybersecurity company Kaspersky and had allegedly been able to monitor hacking efforts by their Russian equivalents.

What the Israeli uncovered was a scheme by the Russian counterparts to scourer cyberspace through Kaspersky for U.S intel (Nakashima, 2017; Perlroth N, 2017). Showcasing how the integrity of cyber security tools can be used by foreign intelligence apparatus, important to keep in mind that these examples detail intelligence work that sometimes is manipulated. However, it can highlight how even the top level of cyber security people in the world are also targetable and the impossibility of guaranteeing the integrity of computer systems (Dupont, 2019).

2.3 DORA

Financial institutions and global economic networks have a range of security concerns that target the financial sector. The consequences of not addressing cyber events and the reliance on central hubs that can be controlled by major states have already been seen in places such as Estonia, where Russia is the prime suspect and now with the war in Ukraine, it looks like the future of cyberwarfare and security risks is already here (Coalson, 2009; Herzog, 2011; Traynor, 2007). DORA or the Digital Operational Resilience Act is one answer or example of how the European Union is trying to make sure that its financial institutions are safe from cyber-attacks in the future. One example of how devastating a cyber-attack can be on infrastructure is the Mærsk case where a malicious software called “NotPetya” cyber-attack infected computers and most famously took down the entire operation of Mærsk in a matter of hours. The software developed by a Russianbacked software company was so destructive that one of the largest shipping container companies operating 1 fifth of the world's container ships had to shut down its operations (Capano, 2021). This is one of the reasons why DORA is trying to stop its financial institutions from getting hit. Moreover, European cyber risks are intertwined with our interdependence with outside states or that has been the case pre-2020. Examples of foreign companies trying to grab onto both US and European internet network hubs are already part of history. Huawei, a global telecom supplier, and phone manufacturer came into the spotlight in 2020 and 2021 after fears that its ties with the China government would allow them to spy on Western countries. Huawei was dropped from 5g infrastructure plans in Denmark and the United States Department of Commerce's Bureau of Industry and Security Entity List in May 2019, following an executive order from then-President Donald Trump that effectively banned Huawei from US communications networks (CISO'enen, 2019; Cerulus, 2021; Keane, 2021). From the perspective of weaponized interdependence, DORA is a measurable example that allows the academic paper to analyze what its impact could be on European cyber security and resilience. DORA fully ties into the idea of weaponized interdependence and cyber resilience thinking. To fully understand why DORA could be a necessary step for EU nations the paper will analyze how cyber resilience and weaponized interdependence tie into DORA and the challenges and issues that might come with it (EU, 2020). The DORA paper is found on the register of commission documents on the European Commission's website (European Commission, 2020c).

At this point, the EU faces a growing number of hybrid threats from adversaries. To reduce the risk associated with hybrid threats it must be acknowledged that no matter how hard we work on identifying and quantifying said threats adversaries are adaptive in their ways. Our adversaries will always find a way to disrupt globally connected information, money, or energy systems in any way they see possible. Therefore, it is important to develop an ability to recover from or adapt to the shifting threats. Cyber resilience is therefore seen as a new evolution in the way organizations and states view and work with cybersecurity and hybrid threats. In the event of a major cyberattack cyber resilience requires actors to have the ability to positively adapt to avoid major losses or issues. The critical challenge here is that digital hacking and infrastructural failure are just a few of the challenges where disruption can trigger significant and lasting consequences for international actors. Furthermore, is a growing and troublesome increase in complexity and range of consequences produced by adversaries. Because of the growing interdependence and increase in centralized hubs, a "butterfly effect" is included in a growing set of challenges where disruption to one system can have widespread consequences on others that are dependent on that specific entity. In the context of weaponized interdependence, the growing threat of cyberattacks, and the centralization of internet hubs the impact will continue to challenge policy, decision-makers, and the EU. Therefore, cyber

resilience is beginning to turn our ability to develop and meet the growing set of challenges in the future. This is exactly where DORA comes into play for the European Union.
DORA is made to standardize certain requirements for financial institutions (Irene Christine & Thinyane, 2020; Linkov, Roslycky, & Trump, 2019; Linkov & Trump, 2019).

DORAs regulatory and legal compliance framework will define managing information and money systems in financial institutions. Creating a better foundation and groundwork for banks to sufficiently protect themselves against weaponized interdependence and adverse cyber events. DORA is a tool against the security concerns of global economic networks and will define the criticality threshold for services provided to financial institutions. An example of the requirements by DORA is that financial institutions must report breaches on their suppliers and service providers as well as part of their contractual obligations. If an organization or company is not willing to accept those terms DORA prohibits it from doing business with them. All in all, DORA determines the terms that financial institutions require from their supplier which makes the entire supply chain cyber resilient (EU, 2020).

2.4 The bank interview

The The bank interview serves as an example of how a chief operational risk manager views and handles the cyber security threat picture at present. The interview was done at The bank where we sat down and talked about a multitude of questions ranging from financial, cyber security, and somewhat political also. This is to give an insight into the interviewee's world and especially two ratios matter in this regard. First, it is important to create an opinion and let the interviewee describe his view on the matter. Secondly, it serves to give crucial insights into the case that otherwise would be hard to get purely from academic sources. To summarize the purpose of a qualitative research interview is to gather descriptions of the interviewee's world concerning an interpretation of that (Kvale, 1998). The academic paper is not a case study of the aid interview but is there to try and exemplify the current issues and challenges that face financial institutions, and our financial security. The interview will also be used to discuss the way financial institutions portray the threat picture they are in and how that fits into the social constructivist analysis also undertaken before the interview, more on that in the methods section.

3. Theory

3.1 Social constructivism

The academic paper takes a social constructivist perspective regarding understanding and concluding how we as people are reacting to the changing dynamic in the international arena and how it might see the impact of cyber resilience on financial institutions. In international relations constructivism argues that the complex web of international relations is not the result of shared assumptions through time or basic human needs. On the other hand, constructivism argues or reconsiders the nature of human interactions. The basic social constructivist approach is based upon that our knowledge of the world, including our understanding of human beings, is a product of human thought rather than grounded in observable external reality. Therefore, what captures the social constructivism approach most is the core concepts; First, is the act or what is labeled as *agency, order, self, relatedness, life span,* along with the social reality and social structures. Individuals are labeled as active participants and *agents*. Furthermore, are the developed and well-known concepts of *norms* and *institutions* as stable and normative *structures* that organize the world. There are arguments for that *structure* lack the dynamics of constructivism and therefore should be reconsidered, however, in this academic paper it is understood in its basic term (Bertucci, Hayes, & James, 2018; Burr, 2015; Onuf, 2013).

This academic paper understands the social constructivist approach as multidisciplinary and as having representation in sociology, psychology, learning and education, philosophy, linguistics, communication, media studies, political science, and most importantly international relations. It is important to understand that a social constructivist approach is a broad approach that encompasses many aspects of human nature instead of narrowing our nature down to a few characteristics. There is not a general or integrated theoretical and methodological framework for the study of all social relations, however, constructivism could be a way of viewing human nature from several different perspectives. This can also be viewed as a negative as it could over-complexify the case that is trying to be understood. Sometimes the best explanation for events is the most logical and easiest. Furthermore, the social constructivist approach is typically used in a qualitative approach and that is also the case in this academic paper. The focus here is on interpreting the complex ways people adopt to make sense of their lives and experiences. Based on their personal and collective interactions on one hand and the other hand their social context of living. These can both be social cultural and historical norms that affect or constrain their actions.

And specifically, resilience and the human thought processes behind those actions is a great question for the social constructivist approach. It should be noted that the social constructivist approach might not be able to give a full answer and understand all possible social behaviors behind human actions, but it might be able to give a reasoning behind some aspects of human relations and if those actions are based on their social, cultural or historical norms (Pricopie, 2020).

The epistemology of social constructivism is characterized by what it sees as knowledge. In its basic form, it problematizes the claim that we call knowledge and our current understandings of the nature of the world and its phenomena. Social constructivism is derived from an objective and importantly unbiased observation of events. Those events are only perceived by those who exist to witness them and by that it also does not argue with the problems in biases. Other approaches in international relations such as realism or liberalism comes are argued to come from somewhat of a biased point of view. This academic paper sees social constructivism as an answer to systemic biased methods in science. In turn, the concept of bias rests upon the concepts of truth and accuracy which also is challenged by the social constructivist method. The solution for social constructivism is, hence, to take an epistemological position of relativism or referred to as perspectivism. This position argues that there can never be one final or “true” position when it comes to accounting and describing experiences. Instead, there are potentially endless amounts of versions of an occurrence. Therefore, there is not a single correct conclusion in social constructivism instead different ways of understanding the world exist. Thus, the academic paper recommends taking an objective, critical and skeptical perspective on the truth and nature of the real world. This is also the reason why it was chosen to analyze the occurrence in world order since the old and already used methods perhaps are somewhat biased towards new paradigms (Burr, 2015).

Historically the constructivist approach is a fairly new paradigm in social sciences and international relations compared to other older and more rationalist approaches such as realism or liberalism. It emerged after 1957 as an alternative approach to empiricism, realism, and naturalism. In the very beginning, it was published by Piaget and his constructivist theory, as stated earlier, that people produce knowledge and meaning based on their life experiences through the mechanism of accommodation and assimilation. Accommodation is the process of changing internal mental structures to consist of external influence. And assimilation is fitting an external reality with internal cognitive structures, or schemas. Later, the constructivist approach became based on the main premise of cognition that allows us to constantly reconstruct the social reality surrounding us. Thus, producing representations of social reality tailored to our social and cultural views and subjective practices. This practice of seeing social realities adopted to our social and cultural views is vital in understanding and using the constructivist approach for the analysis. And in international relations social constructivism has its strengths and weaknesses. At the general level, it is widely recognized that constructivism is a strong approach. In comparison to other approaches such as realism and liberalism, which could also serve as a valuable tool for the analysis of cyber resilience, social constructivism provides an alternative approach to the understanding of norms and ideas that constitute power and interests. However, in this academic paper, the argument is that power is truly a social phenomenon, in other words, norms are not merely confused with regulative and restrictive roles but they possess productive and constitutive effects as well (Goodin & Tilly, 2006). Furthermore, social constructivism adds an emphasis on the "ontological reality of intersubjective knowledge" and the "epistemological and methodological implications of this reality" (Jung, 2019). On the contrary, there are weaknesses with the approach as well. It is generally understood that it invites a sort of criticism as it can be labeled as "selection bias" in some ways. And for those reasons the reader needs to understand that the resources highlighted in the analysis are chosen because they do help to support the thesis and the conclusion, however, it should not be taken as the conclusion. There could very well be other sources that could support the opposite argument (Jung, 2019).

To understand the societal connection between cyber resilience and the way actors see the world, it is important to explore their worldview and how they view the role of globalization. To understand how the thought pattern for cyber has gone from security maximization to resiliencebased. In social constructivism, it is essential to explore the worldview that the actors involved use. In the case of cyber resilience in Europe, there has been a clear shift in norms and what we value as important for our liberal ideals. Doing the "optimistic" years of globalization, where we thought that promoting our ideas to the world through globalization it would mean that others would see what we see through our worldview and adopt our way of life. However, several examples of forcefully pushing liberal ideas and democracy through war and globalization have shown it is not working the way we envisioned it in the first place. The first question to ask could very well be why is it important to have a cyber-resilient act in Europe in the first place? What norm views have changed that now we are suddenly moving away from just securing towards resilience. What is it exactly that happened in Europe that moved us away from the globalist ideals we had before? One example that highlights one side of the argument for a shift in European policies is the year 2019. In 2019 we saw a general shift away from European cooperation with, especially China. It was also the year when the Huawei 5G case unfolded and globalist ideals clashed with security policies in Europe, the United States, and Canada (Segal, 2021). But a more insistent European line towards China emerged in January of 2019. In the European-China policy paper on economic relations from the influential Federation of German Industries, a new perspective surfaced on China and how the European Union should view them. Social constructivism is important and central to understanding how people view others by looking at how they write about them. Words are often a better way of analyzing an actor's view on certain problems and issues, and this social constructivist analysis needs to establish how the European Union is writing about transboundary cooperation and interdependencies. Also, important to note that Germany has a central and powerful position in European financial policies, and therefore, using a German policy paper is a good way of understanding and substantiating a social constructivist approach. The policy paper on China begins by asking "Partner and Systemic Competitor – How Do We Deal with China's State-Controlled Economy?" (BDI,

2019). There is clear wording in calling China a "systemic competitor", which the European Union or Germany has never labeled China as before. BDI advocates for strengthening the competitiveness of the European Union with effective economic policy instruments to take advantage of the State-Controlled economy of China. On the other hand, by looking at the 2018 directorate for Internal Markets, Industry, Entrepreneurship and SME (Small and Medium-sized enterprises) the wording is different. Here European-Chinese cooperation is shed in a different light. China is not labeled as a "systemic competitor" and instead of posing different challenges to how the European Union are challenged by systemic competition because of the differences in our liberal open markets and their state-dominated economy, they advocate for an open dialogue to help better understand Chinese legal and regulatory framework. Especially the use of dialogue is apparent in the latter document, however, as shown just a year after there has suddenly been a shift in tone and wording (The Directorate-General for Internal Market, 2018). Moreover, it feels like there is a clear difference in the way BDI is advocating for the European Union to view China. Instead of playing along with their rules, they argue that the European Union should be able to withstand the pressure of Chinese global market driving abilities. However, the important thing to notice from a social constructivist perspective is how they label China. For so many years the west have played the liberal game as mentioned earlier, trying to force others to become more liberal by interdependencies and globalism. But just as BDI argue there needs to be resilience in Europe towards Chinese power.

This academic paper sees a clear distinction in the way the European Union is shifting toward a more resilient thought pattern by labeling China as a competitor instead of the sole through cooperation and perhaps a bit of fear. One of the reasons why this has gained even more speed in the last year or two is perhaps because of the Corona virus. And how that showcase to the leaders of the European Union our vulnerability to interdependencies and supply chains across the world. And currently, the Russian-Ukraine war has forced the European Union to fast-track the process of letting go of Russian gas. The argument here is that social constructivism perhaps can give a better understanding of why are views are changing. Moreover, also to try and explain the security shift in Europe, perhaps the way we saw China as someone we could cooperate with did not spark the same kind of security feel as when we label them as a "systemic competitor" does. Now are perhaps a fraction more afraid of what China could do if we label them differently. It is a hard question; however, the starting point of the analysis will be the United States as it historically has been a place where the European Union looked towards for security and mostly we followed along on their perspective on it.

4. Method

This academic paper is a research-based paper with the inclusion of an interview undertaken to support the social constructivist analysis and conclusion of the thesis. The data gathered for analysis is primarily peer-reviewed research-based academic papers found on SDU summon engine and google scholar, however, some are also from other internet services. The aim is to produce a real-world knowledge of behaviors and social structures. The methodological approach was qualitative and used because it is most suitable in answering the research question. The social constructivist approach is discussed under the theory sections which includes thought on its validity and reliability as a type of research. Furthermore, to gain a better insight into the cyber resilience of a financial institutions an interview was conducted. It was done as a half-scripted interview through a deductive approach. The interview was conducted at The bank's headquarter. Answers were recorded by phone with consent and then transcribed afterward. Furthermore, the interview was done using an interview guide, which is attached as appendix 2 and the transcript as appendix 1. The first and second part of the analysis is research-based, whereas the discussion used a deductive approach to test the theories and results deployed in the first two parts. The discussion used the findings in the interview, together with the social constructivist perspective findings to analyze and discuss a conclusion. The basis of the deductive approach was to gather evidence of how the interviewee would see and describe his world in cyber security, and specifically to support the social constructivist analysis. The social constructivist perspective and analysis in the academic paper uses a discourse approach to studying communication and meaning in relation to their social context (Hyland, Paltridge, & Wong, 2021; Kvale, 1998; Kvale & Brinkmann, 2015).

5. Historic overview

5.1 of globalization and interdependence

The current wave of globalization seen today and in general international trade kicked off in the 1990s followed by a rapid increase and growth of complex networks of global value chains. But the wave of globalization we see today was not the first one to push through every world border. Back at the beginning of the 20th century in 1919 John Maynard Keynes an English economist, journalist, and financier best known for his economic theories, Keynesian economics, on the causes of prolonged unemployment (Britannica) wrote in his book, *The Economic Consequences of the Peace,* what the impact of the first wave of globalization had on the world. He writes:

> "The inhabitant of London could order by telephone, sipping his morning tea in bed, the various products of the whole earth, in such quantity as he might see fit, and reasonably expect their early delivery on his doorstep, he could at the same moment and by the same means adventure his wealth in the natural resources and new enterprises of any quarter of the world, [and] he could secure forthwith, if he wished it, cheap and comfortable means of transit to any country or climate without a passport or other formality" (Keynes & Cox, 2019).

At this point, globalization had for the first time taken its hold on the world's network of global value chains. Information, goods, and services could be ordered as John Keynes wrote from the doorstep of London homes. One event altered the progress of globalization so much that it was not until the end of the Second World War that the world again could see its networks of global chains progress. It was the First World War, and it produced a profound economic dislocation which included the withdrawal of Russia from world trade after the communist revolution in 1917. Following World War 1 and the events surrounding its international trade, cooperation and progress halted until the end of World War 2. Monetary instability in the early 1920s, new immigration restriction, and the Great Depression in 1929 was some of the events that unfolded because of a recession in progress. This recess in international cooperation and globalization resulted in an outbreak of protectionism in many states. Looking at these events from the perspective we have today in 2022 it can begin to look like history is almost repeating itself. And one thing that especially impacted globalization and the global supply chains was the Spanish flu. Pandemics have a profound effect on supply chains as states must close their border to protect and contain the spread of sickness. This made states have more emphasis on their borders instead of spending valuable money on expanding global trade and cooperation. It is hard to make any conclusion based on this as the events that unfolded around the current pandemic are not completely the same. But for the reader to understand how globalization was impacted in the early parts of the 20th century this understanding is valuable. As globalization started to gain more and more traction in the 1990s so did China as it began its evolvement into the international actor it is today. One of the main factors for China's development was international trading and it looked for many years that cooperation with China and other developing states would through interdependence lead to more and more cooperation and perhaps peace. But now 30 years later China and the US have gone back to the old ways of trade wars between large states. Together with a growing economic discontent in Europe, the US and Latin America's unease in global trade started evolving before the pandemic set in in 2021 (Razin & National Bureau of Economic, 2020).

To understand the ways globalization and interdependence have had a shifting position in the international arena we begin at an event such as the pandemic that showcases the challenges and vulnerability of globalization and interdependence. It is not because the pandemic started the trade war or the weaponization of interdependence between states but from a historical perspective, the pandemic is once again the event that showcases the vulnerabilities of the global network that exists between states. And as soon as those value chains between states are in danger some states begin to look at how to take advantage of those vulnerabilities. That is where the European Commission is coming from when advocating for more resilience thinking in cyber. They are aware that perhaps globalization and interdependence did not have the impact on non-democratic states as we thought and now those states are willing to take advantage of the complex network of global value chains and the higher participation in intra-regional trade. There has been a shift in thinking about globalization and it is the argument that Henry Farrell and Abraham Newman argue in their paper that weaponized interdependence challenges the long-standing ways that international relations experts think about globalization (Farrell & Newman, 2019). From a historical perspective, it compels financial thinkers to think differently about foreign economic policy, national security, and grand strategy for the next century.

5.2 of resilience:

A historic overview and aspects of resilience thinking will help to support the analysis and the reader's understanding of how everything came to be. The general literature on resilience thinking dates back over the past 50 years. The thinking has gone through several stages ranging from the initial focus on the invulnerable and invincible child to psychologists beginning to recognize that much of what seems to promote resilience originates outside of the individual. This is what we see today how the outside influence of the agent is what influences resilience thought. This thought pattern that began 50 years ago led to a search for resilience factors at the individual, family, community, and lately the cultural level. Fleming and Ledogar in their 2008 study on resilience literature conclude that in addition to resilience factors as a feature of individuals there is a growing interest in resilience as a feature of entire communities and cultural groups. This is the basis of this academic paper and the idea that resilience is now used on entire nations and in international relations (Fleming & Ledogar, 2008). Resilience in international relations and security is a thought pattern or a process that for long has been used by actors both internationally and nationally to react to outside threats. Different international relations schools like realism, constructivism, and liberalism all have separate ideas about how actors behave in the international arena. Resilience is on the other hand a behavioral pattern those states have utilized to keep ahead of the curve. And resilience has a lengthy history of practice and implementation for events of extreme consequences and high uncertainty.

Contemporary researchers have contributed to the idea that resilience is a process that introduces different risk features that can vary in contexts. To characterize resilience factors, it is important to view them as a process. The academic paper looks at the different risk factors associated with cyber resilience and financial institutions in a process context. It is important to keep the notion of resilience thinking as a process when analyzing the stated thesis. Fleming and Ledogar have developed to measure and identify resilience factors three main types of resilience: “compensator”,
“protective” and “challenge” models. The model is to be applied to the notion of cyber resilience so that it is better understood how resilience can and is applied in the analysis. (Fleming & Ledogar, 2008).

5.3 of Cyberspace and the challenges, it poses

The history of cyberspace dates to the development of the first computers in 1969 and back then it seemed impossible to imagine a world where cyberspace has the level of influence as it does today. What cyberspace was back then is not the same as today. Back then cyberspace was something only very few people knew and had an idea of what it was. Today, cyberspace is used by every imagined institution, government, organization, and individual. The first cyberspace created was made by the United States and some American universities. The idea was to set up and connect a set of computers in a network that they labeled “Arpanet”. The network allowed scientists from all over the country to send information back and forth. At first, the scientist using the network were all new and trusted each other, however, as more and more people got personal computers it changed and individuals from the outside started joining the network. And then in 1991, the introduction of the “World Wide Web” by Tim Berners-Lee marked the beginning of a new era in human technology and communication. It is a system for connecting files to each other across the internet, allowing users to easily explore a vast world of information, often described as “cyberspace”. (Encyclopædia, 2020; Paloque-Bergès & Schafer, 2019).

Even though today everyone is familiar with the World Wide Web back then it laid the foundation for future technologies. And today we see how its exponential growth has expanded into a new sphere of modern life where users can interact with each other and share information. Through the internet government, businesses, and all types of organizations can gather more information and operate at a higher speed. However, as it is already understood cyberspace created a range of challenges for its users. In the beginning, the internet was created by members of a community that trusted each other with good faith, today that has completely changed and the need for cybersecurity is greater than ever. The internet has in many ways made the life of users much easier but it has also exposed us to a world of danger. This is where the European Union and governments see a set of challenges posing against our fundamental security, for example, centralization, weaponizing interdependencies, cyber security responses before, during, and after an adverse event, and so forth. As mentioned previously the world has seen examples of what can happen if cyberspace is attacked by adverse entities, i.e., cyberattacks on critical infrastructure. With cyberspace's short history it is sure to say that we have not yet seen the full effects of adverse cyber events

5.4 of DORA and the EU Cybersecurity Strategy

The historical perspective on DORA is mostly to give the reader an understanding of where the European Union is coming from when they proposed DORA as a new legislative. The history of DORA does not go far back in time; however, the EU has seen its share of cyber-attacks from independent groups and states in the last decades. And, since the events in Tallinn, Estonia experts and other institutions have not understated the importance for the EU to tackle future cyber-attacks better. The DORA legislative comes out of the Cybersecurity Strategy that the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented in 2020 (European Commission, 2020b).

6. Analysis

6.1 Cyber resilience and financial institutions

To understand and analyze how financial institutions can enhance cyber resilience and what the challenges for financial institutions are. The analysis takes its starting point from the international arena of global power. Then after it will describe and analyze DuPont's five dimensions of resilience to give a fuller picture of cyber resilience and the challenges associated with it. Cyber resilience and more specifically weaponized interdependence start at the level of hegemonic power where the United States for many decades has been at the top of the ladder. In the international arena the United States has allowed itself to utilize financial power across the globe and in many instances weaponized the interdependence onto states through global economic networks. The analysis must explore why financial institutions are challenged by weaponized interdependence. Furthermore, why the European Union are advocating for more cyber resilience and protecting European financial institutions from adverse cyber events. To start this the paper will outline how financial institutions and the entire financial sector is dependent on the internet and other aspects of globalization. These dependents highlight the need for cyber resilience but also how powerful states can take advantage of the centralization that has been ongoing for at least two decades.

The United States has for many years used its position as a global hegemon to utilize its power across the globe through global economic networks. The reason why this is important is that it highlights why weaponized interdependence is an important factor for European financial institutions and overall security. One example of The United States taking advantage of its power position over global networks was in 2020 when it imposed sanctions on aviation companies for their work with Iranian airlines. This is to not allow them to sell aircraft or repair parts to Iran. The United States and Iran have a long history of sanctions against the country for their nuclear program and support of groups considered terrorist groups by the United States (AP, 2020). Russia's Gazprom echoes the same power as the United States has shown to be able and willing to use. Krutikhin's article detail and exemplifies how Russia is using weaponized interdependence through gas pipes to gain leverage power over gas-dependent countries (Krutikhin, 2021). The important thing to notice in the United States case is how they use their power over aviation networks to impose their power over Iran. This idea of utilizing and weaponizing interdependence is not a new concept and as exemplified the United States is not the only one that is using these tools. The role of global networks is now greater than ever, and globalization have fostered and advanced a network of economic, informational, and physical exchanges that are extremely hard to unravel now. Thus, the outcome of this is that global economic networks have generated a higher amount of security consequences than previously seen. The basis for this is that globalization has increased over time the interdependence between states that were previously relatively autonomous. The profound effects globalization has had on our society are seen in many different aspects of it, this can be in finance, information, goods, or energy. The financial sector in which this paper takes its perspective has become intertangled and dependent on international messaging networks, which are key to financial institutions. Financial institutions use international messaging networks to arrange transfers and communicate with each other. The internet, as described previously has had a tremendous effect on communications throughout the world and the financial sector is no different from others. They rely heavily on the internet and the services it provides for institutions. But what has the outcome been for the United States that was shown as an example of weaponizing global finance? Oatley argues that it has produced mixed results. On one hand, it denied terrorist groups access to traditional channels of financial transfers. It is noted that commentators have concluded that it did play a role in multilateral negotiations with North Korea and Iran. On the other side at the point of writing his article Oatley concludes that it did not force Russia into acting the way the United State wanted. Therefore, not producing the desired result. A year later given the current situation in Ukraine, Russia is again under financial pressure and at this current point, it has not forced Russia to back away. However, the real impact of the sanction is probably felt by the people and not the state. Weaponizing interdependence is a tool for states to use and that powerful ones tend to take advantage of their position in the global international arena. (Farrell & Newman, 2021a; Oatley, 2021)

For financial institutions in Europe, the issue for them is that global economic networks are centralized in hubs, thus, making the European financial institution vulnerable. What we are seeing in finance and global economic networks is the notion of large international institutions becoming crucial intermediates in global financial networks. They are acting as middlemen across an enormous number and variety of specific services and goods. These intermediates just to name a few could be Google, Citibank, Visa/Mastercard, or financial clearinghouses. What this is trying to tell us is that the global economic networks that serve European or Western countries daily and the foundation for our monetary security are centralized in major international companies. These companies are not scattered around the world in randomized locations these are mostly located in the western dominated countries and most other nodes, or "hubs" are dependent on them. These centralized hubs are a product of globalization and rich people getting richer by centralizing control in a few major companies (Farrell & Newman, 2021a). However, the effect on European security is that by centralizing all these services in a few "chokepoints" we make our financial infrastructure more vulnerable to outside adversary attacks. And by building centralized networks we unintentionally provide states from the outside, the tools to leverage their political as well as economic influence over our borders. The conclusion to this could be that our financial-economic networks might be vulnerable to outside influence and protecting them is vital for our security. And as explained states can weaponize economic networks to their advantage and use them against us. The need for security and resilience could be a solution to solving the security issue for European financial institutions because global economic networks such as financial communications, supply chains, and the internet, which have been largely neglected by international relations scholars are at the heart of the European security issue (Farrell & Newman, 2021a; Oatley, 2021). And by looking at examples such as the Huawei 5G internet infrastructure deal in Canada starts to show what could happen if foreign powers do get their hands on critical infrastructure (Young, 2021). This could show us why European states are so afraid that their financial institutions are vulnerable to outside attacks. Those power displays could both show as a direct attack on financial-economic networks, but they could also be from the inside where outside countries like China get a hold of key infrastructure deals that they then can control as they like.

Globalization has transformed the liberal order, by moving the action away from multilateral interstate negotiations and toward networks of private actors. And together with the topography of the economic networks of interdependence that intersects with domestic institutions and that therefore shape norms to coercive authority. If states and organizations are to secure their networks of private and national actors there clearly must be applied a new thought pattern to security. A new more compelling understanding of globalization and power together with cyber resilience could be the answer but what is the significance of cyber resilience in financial institutions. A fair question to ask is there a need for cyber security and resilience in financial institutions today? The quick answer to that might be obvious and many would answer yes because we are highly dependent on the function of our financial institutions. The next section will go deeper and examine the need for cyber resilience in the financial sector. First highlights the different types of threats that target financial institutions and then the impact they can have on critical infrastructure. DuPont's article on cyber resilience in financial institutions is a good tool and place to start the analysis of cyber resilience as it goes into the threats and vulnerabilities of financial institutions.

As stated before it has become evident that our financial institutions are becoming more vulnerable to a growing list of effects that will affect institutions' ability to maintain security and uptime. With a growing dependence on digital technologies, today's financial institutions and organizations that secure critical infrastructure are particularly vulnerable to the effects of cyber activities. Whether it be technical failures, human errors, or natural disasters the digital infrastructure is more vulnerable than ever before. Especially vulnerable are the digital assets of financial institutions which are highly sought after by cybercriminals and states that seek to take advantage of said vulnerabilities, to perhaps destabilize another state or organization. And according to the Carnegie Endowment for International Peace which keeps track of the evolution of the threat landscape in cyber incidents. They do not track every single cyber incident obviously because there are so many that it would require a large amount of information, but they target cyber incidents that have shaped the cyber landscape since 2007 based upon the Cyber Threat Intelligence unit of BAE Systems. Since 2007 they have tracked approximately 200 major cyber incidents involving financial institutions (CARNEGIE, 2022). And is apparent that a growing number of cyber incidents involving financial institutions are taking place and the reaction towards the trend is a growing trend towards legislation concerning information and communication technology in organizations and states.

Carnegie has also issued a policy paper, "The European Union, Cybersecurity, and the Financial Sector: A Primer", here Krüger & Brauchle conclude that compliance is one of the main drivers for cyber resilience, and a prudent and consistent regulatory strategy can help to ensure the necessary baseline insecurity across the financial sector to mitigate institutional and systemic risk (Kruger & Brauchle, 2021). So, it is evident that there is a growing trend toward cyber resilience in the financial sector but what kind of cyber-attacks or weaponized interdependence threaten our institutions?

The most common and known threat against financial institutions is cybercriminals that are motivated by financial gain. This is the threat that people mostly hear about and there is a growing number of cyberattacks that target bank clients, business customers, and core bank systems. The evolution of these attacks and the reason why they are the most obvious is the quick pace of innovation in malware technology and software. The tools for hacking and going after the customer's money have become increasingly affordable over time allowing cybercriminals more easily to deploy attacks. The SWIFT Institute, the institute that has built the complex technical infrastructure of our financial institutions, issued a report in 2017 that described how cyberattacks are more complex and sophisticated than seen before. And with the new technology, also means that criminals do not need the same kind of technical skills as before, allowing more people actively be cybercriminals (Carter, 2017). And it is not only criminal groups that do these kinds of hacks state-sponsored groups are highly known for their hacking based upon financial gain. Both Russia and North Korea have shown an example of how state-sponsored groups carry out hacking efforts for monetary gains. An example of this is the Lazarus Group from North Korea which stole around 600$ million dollars from a video game company that held their investments in cryptocurrency institutions in February of 2022. This comes from the FBI which is blaming the North Korean government and the Lazarus Group for carrying out the cyber activity (FBI, 2022; Lyngaas, 2022). It is known that state-sponsored attacks are of higher importance because of the notion that those groups have more resources as states are more willing to get the results and effects of their attack. These attacks are also more challenging for financial institutions to defend against on one side it is because that statesponsored groups have more expertise and resource but also more time to find the right approach or vulnerability in systems. Another reason for cyber-attacks can be ideological motivation and it is seen before that “hacktivist”, a word for both hack and activist, are behind cyber-attacks. One of the most famous hacktivist groups is Anonymous which has made several famous hacks against targets they believed were not acting appropriately based on their idea of society and democracy. For example, they are famous for their support of WikiLeaks, which they later turned around on, and during the invasion of Ukraine, they hacked several Russian governments system and national tv so they could counter the disinformation campaign by the Russian government (Chirinos, 2022; Halliday, 2012; Tidy, 2022).

However, attacks from ideologist motivated cyber groups have shown to interfere with or stop financial institutions in their day-to-day operations. What financial institutions are more worried about is state-backed groups that operate behind the curtain and off the grid. Their approach should not be dismissed and in the future hacktivist groups may manage to disrupt the services of a financial institution. Furthermore, on the type of cyber-attacks financial institutions face, the last two threats financial institutions fear are from third-party entities in their supply chain and insiders in the organizations, which can advantage of vulnerabilities or distract operations during attacks. Especially the first threat of third-party entities is risky for financial institutions, one example of this was in the media not long ago, which is the SolarWinds incident. SolarWinds was the subject of a massive cyber security breach that spread through the supply chain. The company itself is a major US information technology company that had clients such as Microsoft and top government agencies. Hackers got into the company's systems and added malicious code to the company's software. From here the malicious software spread to SolarWinds clients and made it possible for financial institutions or others alike to be disrupted (Jibilian, 2021). Securing the supply chain is highly important for financial institutions and the EU as this is appearing to be an easier way into the security systems of financial institutions (Dupont, 2019). To understand the reason why it is important to know the threats financial institutions face. It would be easier for the reader to understand the analysis if it explored what kind of weaponization adverse states can take advantage of.

Moreover, it is not only the direct cyber-attack tools just exemplified but there are multiple dimensions to resilience. They range from different interdependences on third-party organizations to internal notions of adaptive resource use. These interdependencies are risk factors and shape the risk profile for financial institutions. Financial institutions are aware of the risks associated with cyber disruptions. The International Monetary Fund issued a working paper on cyber risk for the Financial Sector: A Framework for Quantitative Assessment, which described scenarios on the key threats to financial stability. The author Bouveret presents a framework for assessing cyber risks. The paper gives a good picture of how the outcome of a major cyber event could affect financial institutions. Although as he describes himself he acknowledges the incomplete and introductory nature of his model, the implications for financial institutions are alarming and show the risks associated with a major adverse cyber event. It could explain why financial sector executives rank cyber risks as their main operational risk concern. In his report, he describes how an adverse cyber event could result in 20% net income losses for banks in an unbelievably bad scenario. Not to go further into it, the important notion is that such an event could have devastating impacts on the function of the financial sector (Bouveret, 2018).

The next section goes deeper into the aspects of cyber resilience and its dimensions of it. The first and earlier paradigm in cyber security was a time when protection was based on the inadequate thought pattern of "prevent and protect" (Raff, 2013). Today cyber resilience is challenging the thought and perspective on securing digital infrastructure. Instead of only deploying a thought pattern that is based on protecting, cyber resilience takes more dimensions into account and bases its thought pattern upon scientific research that in theory should allow a financial institution to be more resilient toward adverse cyber events. Thus, it is important to explore the dimension of cyber resilience before going into the aspects of how financial institutions are weaponized through interdependences and exploring how not to become a panopticon of adverse entities. If a financial institution is to become cyber resilient against the weaponization of interdependencies, there are several principal factors in growing one's ability to reduce the occurrence or impact of disturbance through resilience. The challenging part with cyber resilience is that the very intricate nature of our society and the complex system that financial institutions interact with have an array of geographical, temporal, functional, and technological dimensions that must be considered. Because of the overly complex nature of resilience Dupont argues for a set of five dimensions that are a summary of the literature on resilience thought (Dupont, 2019). The literature contains many detailed models that attempt to contribute to the notion of how to enhance organizational resilience. To understand resilience better the analysis will go into the dimension of cyber resilience and what the challenges are with each of them. Some of the dimensions are in line with the notion of weaponized interdependence and some are more internal factors, however, both perspectives serve to give an understanding of how cyber resilience can be enhanced and the challenges that come with them. Dupont's five dimensions are: Resilience is… *dynamic, networked, practiced, adaptive,* and *contested* (Dupont, 2019).

Resilience is dynamic: It is clear and in agreement that in the literature resilience requires an extended chronological scope that includes activities before, during, and after an adverse event. This is done through a clear and precise process in which organizations prepare themselves notoriously so that they can withstand the effect before, during, and after. The process is a cyclical and cumulative process where organizations confront themselves in advance with a variety of risks that vary in severity and frequency. Furthermore, organizations should deploy protective technologies and policies that can reduce their exposure to the risks associated with their sector. While also implementing detection and response protocols that can facilitate the ongoing use of their services during an adverse event. Meanwhile, also mitigate the negative impacts and adapt their systems and procedures to absorb what they learn from the ongoing negative event. The timespan of these events can both be measured in days, weeks, or months; however, it is important to consider all the different dynamics when dealing with adverse cyber events (Bodeau, Graubart, Picciotto, & McQuaid, 2011; Dupont, 2019). Overall, there are many challenging aspects with emerging new spheres of power such as the cyber. However, it is important to research and understand the historic perspective on cyber resilience before utilizing its effects on an organization. Before the process deployed by a financial institution can be effective the process before must be at a high enough level that they are ready to respond during an adverse event. However, it can be a challenging feat, just by looking at other cases such as the Mærsk case where the malicious software was built upon leaked software by the arguably best and well-funded cyber agency in the world the National Security Agency in the United States (Capano, 2021). The conclusion to it is that it can be very easy to point out that organizations need to prepare before, after, and during, however, the reality can be much more complicated than they expect. Although, it makes sense for financial institutions to deploy processes that can withstand or at least make sure that the effects of adverse events are as small as possible.

Resilience is networked: Visualization of decision-making in organizations and financial institutions should not be limited to a narrow internal process where decisions are made solely alone. A resilient financial institution should be able to broaden and share its decision-making with other institutions to communicate and contribute to the internal decision-making process. Internally resilient organizations should develop collaborative ties across a business or functional units that can facilitate communications during critical events. The complex and socio-technical system that modern organizations exist in should be reflected in the way they manage resilient thinking. Organizations today exist as mentioned in this complex web of independence between suppliers, intermediates, and clients that hand constrain them and enable them. Resilient thinking must not be a constraint to isolated thought patterns where each entity in the supply chain thinks of themselves as alone in their commitment to security and resilience. Resilience cannot be fostered in this isolation, and it must be active and strongly correlated in a dense network of intra- and inter-organizational linkages that rely on trust, resources, information, and expertise sharing (Dupont, 2019). DORA specifically touches upon this dimension as it tries to enhance the level at which financial institutions communicate and share intelligence. This dimension of resilience thinking is especially critical for those organizations that engage in what Dupont label as "transboundary crises," which he defines as "adverse events that affect multiple jurisdictions, undermine the functioning of various policy sectors and critical infrastructures, escalate rapidly and morph along the way." Externally financial institutions develop a set of diversified ties between strong and weak intermediaries. This could allow them to maintain a high level of awareness, flexibility, and access to shared resources, however, this is again also a weak spot for resilient thinking and financial institutions. The supply chain is an important key component for security and if one intermediate is vulnerable it could endanger the whole economic network. And as Farrell and Newman argue that the centralization of network hubs can further endanger parts of the financial network towards greater insecurity. It could allow other entities to push their power through panopticons that are placed as intermediaries and, therefore, allows for the weaponization of interdependence. The challenge of networked resilience is an important notion for a transboundary institution such as the European Union. Thus, it could be argued that this is an effect of globalization, whereas the transboundary nature of our public and private institutions has transformed our society in such a way that we are highly dependent and interconnected with each other. Furthermore, it poses a challenge for administrative mechanisms to use cyber resilience in adverse events. And with the centralization of hubs, our financial institution needs to be able to work together highly efficiently with each other in a way that is standardized and secure. Ansell, Boin & Keller further back up this claim in the academic paper "Managing transboundary crises: identifying the building blocks of an effective response system." The conclusion on the challenges faced by crisis managers during a transboundary crisis is that the challenge is not any different from a "normal" more localized event. However, what sets transboundary crises apart is that they create a need for extreme adaptation and unprecedented cooperation under conditions in which these are most difficult to achieve. Moreover, they conclude that the response to a transboundary crisis requires a specific set of organizational and procedural tools, such as analytical capacity, surge potential, coordinated behavior, and special authority arrangements (Ansell, Boin, & Keller, 2010). This part of resilience thinking is touched further on in the last part on DORA and the The bank case. Both DORA and the The bank case touch on the importance of especially information, expertise, and trust sharing. Those are vital parts of both DORA, and the way The bank might think about it, but more on that to come (Dupont, 2019; Farrell & Newman, 2021b).

Resilience is practiced: A important factor in handling an adverse event is achieving a high level of competence that includes developing an intimate understanding of the theory and history of both cyber-attack events but also the history of cyber and panopticons. Dupont argues that it is not enough to just expertly plan your actions in the case of an adverse cyber-attack you should be able to combat a high level of uncertainty. Thus, it is important to remember that even though a financial institution has planned itself for a cyber event, that planning is based upon earlier events but there is a risk that the next event might not have any or very little resemblance with what will happen. Therefore, for financial institutions, the way they combat that is to develop a high level of sensemaking skills, surge capacity, interpersonal trust, and dependable institutions ties. While resilience is a factor and attribute that cannot be improvised during an adverse event the skills of those managing the crisis are essential to supporting resilient action. The important thing for managing these events is to set up parameters or structures that put minimal boundaries on managers so that they can think during a “turbulent task environment”. The structures are both social and technical parameters in the sense that managers must have a wide repertoire of knowledge of both the social interactions with other internal bodies in the organization. Thus, they can communicate extremely efficiently during an adverse event, and this is something that needs to be trained beforehand. Furthermore, they need to have a technical understanding of a cyber-attack and the financial institution. Also articulating under what conditions to train and practice under it can become a key component of any financial institution’s cyber resilience. Dupont argues that this will level the resilience of an organization by creating a balance between structures and creativity during an adverse event. One of the biggest challenges in the dimension of practiced resilience is that the resilience of that institution is only as good as the knowledge of the people and the training they get. Studies were done on other adverse events where participants must think fast, creatively, and under certain boundaries, the way to overcome and think during an adverse event might be best done through “startle and surprise” training and practice exercises (Dupont, 2019; Landman, Groen, van Paassen, Bronkhorst, & Mulder, 2017).

Moreover, a challenge that would stress financial institutions is something different and more modest: that holding together an apparatus is work, and that more attention needs to be paid to how apparatuses of security fall apart, fail, are disrupted, or are held together by specific and careful consideration of what these material and contingent relations mean. The manager's role is specific and important in having the right knowledge and understanding of how his or her institution is put or held together, however, there are challenges that they face in knowing the specific and careful considerations of what their apparatus of security is held together by. But the supply chain is challenging this notion that they are not only responsible for their own set of security anymore inside their financial institution they are now also threatened by the security of their supply chain. This is an extremely hard challenge and again DORA is looking at ways to combat this, but it is a challenge (Adey & CISO'enon, 2012). Furthermore, one of the benefits and the other side challenges of this dimension is the notion that rehearsing these scenarios help strengthen and provoke the cognitive response. This can range from both exercising existing knowledge but also a reassessment of existing knowledge. However, on the other side badly rehearsed, designed, and executed rehearsals generate boredom and a dangerous satisfaction that undermines true organizational resilience and supports a fake feeling of preparedness (Bodeau et al., 2011; Dupont, 2019)

Resilience is adaptive: Organizations that are prone or vulnerable to cyber-attacks are not adaptive in the way they can relocate resources quickly. An important aspect of resilience is that organizations can flexibly reallocate resources and have developed a plan to improvise and delegate decision-making better in the case of an adverse event. Originations with a culture of improvisation and delegation are better to face unexpected events. The challenge of preparing an organization for an adverse event is not easy and requires a great deal of adaptivity both in form of training and resilience. To achieve the mentioned attributes and enhance the dimension for a financial institution or alike there needs to be a focus on specific conditions that function to promote cyber resilience. More specifically, in cyber security adaptivity, flexibility and responsiveness are achieved through redundancy and diversity. In cyber security, redundancy refers to the availability of "multiple protected instances of critical resources (information and services)", while diversity defines the "use of a heterogeneous set of technologies to minimize the impact of attacks and force adversaries to attack multiple different types of technologies" (Bodeau et al., 2011). The challenge with resilience that diversity minimizes is the dependence on a single technology or service whose failure may prove devastating for an entire sector or organization. Going back to Farrell and Newman's weaponized interdependence they talk about avoiding centralization in cyber "hubs" or nodes. This is the same deal that Dupont touches upon with his adaptive dimension of resilience. It is a profound challenge for financial institutions and the European Union to avoid this mistake and diversify its financial services and technologies. The same goes with redundancy as it leverages an organization's possible tools by enhancing the number of resources available during a time of strong increase in needed capacity (Dupont, 2019).

The challenge for financial institutions is to try and steer away from an environment where performance and efficiency are considered the supreme method and advocate for the conservation of more generalized resources that may be shifted towards management and alike to be applied when an adverse situation unfolds (Dupont, 2019). This is a challenging dimension for many organizations and in the case of an adverse event there needs to be a focus on the dilemma, and it might explain why some organizations find it difficult to create resilience in the first place. And if financial institutions find themselves in a position where they are being leveraged by an adverse panopticon there needs to be a mechanism in place that can withstand that kind of power. You see in the SolarWinds example where it was extremely hard for the supply chain involved to be able to foresee that kind of panopticon but the ones that withstood it best were also the ones that had the best adaptability in the crisis management of that situation. The organizations with the best resilience display a higher level of adaptive capacities not only during but also after an event. They can deploy basic operations faster and restore destroyed equipment. Furthermore, they are also able to learn and identify improvements in their systems and produce and enhance their level of preparation against future events. It is an optimistic perspective on resilience thought; however, the best resilience should still be aware of not creating a false sense of security even though an organization feels that it has everything under control. It is just until a future event hits that they are not ready for. Sometimes it can be the most unexpected events that damage or interfere with services that they should be prepared for. An example that showcases this was at the start of the Ukraine-Russia war where the United States and the United Kingdom now say that have proof that Russia engaged in a cyber measure that caused internet outages for several thousand Ukrainian customers, it could be argued that the real target was to damage the internet capabilities of the Ukraine military. However, what also happened because of the attack was that thousands of other internet modems were damaged beyond repair in the attack, meaning that windfarms and internet users across central Europe were affected by what could be labeled as a military attack under international law. ViaSat themselves have said that thousands of modems were damaged in the attack however, their satellite and core infrastructure were unharmed physically (Vallance, 2022). For financial institutions and key infrastructure, it displays how vulnerable they are to attacks that are not directly targeted them but also, what the capabilities of adverse states are at this given point.

It is indeed a major challenge for financial institutions to be adaptive to these instances and the right preparedness could give them a higher level of resilience. Furthermore, it also exemplifies how financial institutions should not be dependent on global networks that are centralized in such a way that it makes them vulnerable to cyberattacks.

Resilience is contested: For organizational resilience to prosper the dilemma of a performance in favor of rationality that seeks to increase productivity more than anything else and a resilience-oriented approach that requires compromises between efficiency and adaptability. The last dimension entails the hurdles and struggles that come with enhancing organizational cyber resilience. One thing that very well describes resilience is the lack of resources and time that sit as one of the main barriers towards more resilience. The costs and general effects both at the internal and also at the international level is to be considered too high or simply disproportionate in comparison with the risks they seek to address. At the internal level, an organization's mind finds it unsuitable in their current situation to deploy several dimensions of resilience to avoid future hazards, however, it might not be affordable for all to do that. It can be costly to pay for resilience as an organization must have the financial possibility to pay the support costs of having to facilitate the effective use of their approach, which may lead to greater financial costs. Furthermore, at the international level, it is apparent that the risks of cyber-attacks are greater than the costs associated with cyber resilience

(Dupont, 2019). David Sulton is the author of an academic paper on “Business continuity in a cyber world: surviving cyberattacks” he argued and concludes that the need for business continuity is far greater than what the costs of cyber resilience currently are (Sutton, 2018). As the paper has been mostly focused on the international level but briefly touched on the organizational level of cyber resilience, it is more interesting to look further into what challenges are for a financial institution with cyber resilience and weaponized interdependence. The five dimensions of resilience all entail each of their challenges in enhancing cyber resilience and at the end dealing with the notion of panopticons and alike. However, the last dimension here is what tells us about the problems with cyber resilience. The increase in uncertainty characterizes financial institutions and the cyber landscape at this point. And even though financial institutions invest heavily in cyber security measures cybercrime is still on the rise, further fueling the uncertainty and insecurity in the sector (Ambore, Richardson, Dogan, Apeh, & Osselton, 2017). IBM's *Cyber Resilient Organization Study* from 2021 tracks the ability of organizations to achieve a strong cyber resilient security posture. With over 3.600 IT and security professionals surveyed it is a great tool for details into the current landscape. Highlights of the study highlight that 51% of respondents reported a significant data breach, 61% of organizations paid a ransom on a ransomware attack and 74% of organizations reported inconsistently applying their CSIRP (CSIRP is a "computer security incident response plan"). The

conclusion of the study details an increase in both the volume and severity of cybersecurity incidents over the past 12 months according to 67% of respondents and of the respondents surveyed, 51% sustained a data breach over the last 12 months and 46% experienced at least one ransomware attack over the past two years. The study also details the costs to organizations. One example highlighted in the study is a great showcase of how weaponized interdependence threaten technology networks because of centralization: "One publicized ransom payment made in 2021 involved a large U.S. refined products pipeline system. DarkSide ransomware only encrypted files on the pipeline's IT networks. However, the attack had the potential to spread to the operational technology network. The company made the decision to shut down the OT network as a precaution, leading the attack to have an operational impact and ripple effects throughout the oil and gasoline supply chain" (IBM, 2021). This is exactly the kind of problematic events that weaponized interdependence and panopticons deal with and especially why the European Union is implementing financially resilient acts in cyberspace. Even though in this particular case the DarkSide group claimed that they were only after money and had not intended to create societal problems in that regard (IBM, 2021). To summarize resilience is a congested part of the risk management narrative. As the IBM survey showcase, the pressure on organizations to combat resilience is very apparent, however, there are competing narratives on risk management. The organizational attitudes toward collective resilience battle with each other, and there further challenges for cyber resilience can emerge (Dupont, 2019).

Financial institutions are vulnerable to centralization and weaponized interdependence through intermediaries and supply chain chokepoints. Additionally, it is because of the complex and socio-technical system that modern organizations exist. Financial institutions can gain enhanced levels of cyber resilience through Dupont's five dimensions. However, it requires a high degree of organizational structure, knowledge, and funds to secure against modern threats from both nonstate- and state-sponsored actors.

6.2 Social constructivist perspective of cyber resilience, weaponized interdependence, and DORA

First part: The United States of America's national defense summary (NDS) and view of adverse states from the perspective of future challenges.

To begin the next part about social constructivism on financial institutions and the way weaponized interdependence, cyber resilience, and DORA is constructed, the best place to start is debatably that of the United States. It is no secret that the European Union in many cases looks to the United States on how they view, portray, and argue their points of view on how their enemies or adverse actors should be viewed. The second part of the analysis takes its starting point in the National defense summary by the United States which describes how they view the complex global security environment. The national defense summary is a good starting point to understand how western powers view our "systemic competitors" Russia and China.

The National Defense Strategy Summary is made up of 5 parts, introduction, Strategic Environment, Department of Defense Objectives, Strategic Approach, and conclusion. Each of the parts entails a different aspect of strategic defense for the United States and tells something different about how the United States views its opposition and the security situation although it is 4 years old (*Summary of the National Defense Strategy*, 2018). The Biden-Harris administration has just announced on March 30th that their National Defense Strategy is officially done and issued to congress for review. The only official paper there is on their strategy is a "Fact Sheet: 2022 National Defense Strategy" (*Fact Sheet: 2022 National Defense Strategy*, 2022). However, by comparing parts of the fact sheet with the 2018 National Defense Summary a good understanding of the United States' perspective of weaponized interdependence and cyber resilience.

The United States creates a narrative about the international world order as a downfall. They characterize their military power as an "atrophy", a medical term for the progressive degeneration or shrinkage of muscle or nerve tissue. Creating a firm picture of a military not in the best shape (Merriam-Webster, n.d.). Moreover, they create a negative picture of the international arena as a situation where they are "facing increased global disorder, characterized by a decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory" (*Summary of the National Defense Strategy*, 2018). The perspective the United State have on this is marked by a negative attitude to the situation they are currently in, they are stating that they acknowledge they are facing greater competition internationally. They say this by stating the primary concern in the U.S national security is not only "terrorism" but also "inter-state strategic competition" (*Summary of the National Defense Strategy*, 2018). Moreover, the next part begins by labeling what they probably believe is their number one competitor internationally as has been described earlier China is for the first time labeled as a "strategic competitor". Furthermore, they create a picture of them as using "predatory economics" so that they can intimidate their neighbor's. Since the end of the cold war there has not actually been a competitor to the United States in the sense that the United States sees them as being able to compete against them. The picture they are not creating is that China has progressed so far now that they are labeling them as a new global power competitor to them. However, they do not describe them as a competitor with the same ideals as they describe them as a "predator", meaning an entity that abides by natural laws in some way and is not following what people in the west label as modern ideals. What the United States is doing is creating a clear distinction and description of how they view China now. Furthermore, they describe Russia, North Korea, and Iran as states that do not follow international law, violating borders and pursuing veto power over the "economic, diplomatic, and security decisions of its neighbors" (*Summary of the National Defense Strategy*, 2018). The United States is creating an image that instead of relying on international cooperation is marked by a higher degree of international struggle. They argue that they need to create a more "lethal, resilient, and rapidly" innovating Joint Force in coalition with their allies and partners. The same connotation is used to create a picture that the United States and its allies are in clear need of each other to create resilience towards adverse states. They label the modernization of a joint force with allies in a way that says that instead of promoting liberal ideals now they rely on "peace through strength" (*Summary of the National Defense Strategy*, 2018). A clear distinction between earlier ideas of peace through interdependence. Moreover, the National Defense Strategy is very occupied with the thought of Chinese influence in the world. They describe how "China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage". This goes in line with the idea that globalization is on a downward trend and instead the United States tries to paint a picture that China is taking advantage and they do not care about liberal ideals through interdependencies and cooperation. Instead, the United States believe China uses predatory methods to establish interdependencies on neighboring countries to then take advantage of them through the weaponization of interdependencies. An example of Chinese expandatory methods and strategy is the “belt and road initiative”. Ai Weiei a leading contemporary artist, activist and advocate of political reform in China and a journalist from The Guardian argues in his article that China’s predatory methods “is China's counterattack in a global game of chess” (Weiwei, 2022). And in many ways, the United States' views of China are pictures in their decision and wording of the international security picture in their NDS.

The European Union’s perspective is very much shaped by that of the United States, and they also feel the power of predatory methods of the Chinese state. This serves as a good understanding of European resilient policies and why they talk about more resilience. Furthermore, the United States also describes in the strategy other changes in the strategic environment that they see have happened because “China and Russia are now undermining the international order from within the system by exploiting its benefits while simultaneously undercutting its principles and “rules of the road”. The picture the United States and its allies tried to create after World War 2, through a free and open international order to better safeguard liberty and people from aggression and coercion, has perhaps failed (*Summary of the National Defense Strategy*, 2018). That is the construction the United States is pushing in 2018 and the European nations are closely monitoring this picture. The National Defense Strategy also talks about new emerging technologies as something that will
“change” society. The realm of cyber have several mentions in the summary and for European states, it is a high priority also. The United States mention the fact that the security barrier to new technologies shave been lowered and expanded allowing more actors entry into cyberspace. Lastly, the 2022 fact sheet is very much like the 2018 fact sheet to quickly understand the general arguments the United States still believe that it should act to sustain and strengthen deterrence with the Chinese state as there are still their most “consequential strategic competitor”. Russia still poses an acute threat as their argument is because of their “brutal and unprovoked invasion of Ukraine”, which is probably very much aligned with European opinions now. Furthermore, the United States describes that there is a need to increase resilience as they label it “our ability to withstand, fight through, and recover quickly from disruption” (*Fact Sheet: 2022 National Defense Strategy*, 2022). This serves as a great understanding of how the picture of European resilient thought is created and sustained as they look to the United States for guidance as they have done for decades now. Furthermore, the European Union issued a press release

Second part: Social constructivist perspective on European cyber resilience and weaponized interdependence

To summarize what was described the European Union looks at the United States for guidance on how they view their strategic, defense, and resource priorities. The highlights are that the United States is looking to increase its resilience towards adverse states and this academic paper would argue that so is the European Union largely because the United States is doing it. However, the European Union has also witnessed certain events that are provoking a reaction toward more resilience. Some examples of this are the Tallinn cyberattack, which showcased some of the power and effects a cyber-attack can have on nations (McGuinness, 2018). Forwarding to today the events in Ukraine are also pushing both the United States and the European Union towards more resilience. The question that this academic paper tries to ask is “why is the European Union increasing cyber resilience and security?”.

The European Union is pushing for more and more resilience-based actions, they are trying to make sure that they are capable and can “absorb change and disturbance and still maintain the same relationships” as Hollinger 1973 described it (C. S. Holling, 1973). From a social constructivist perspective, the parameters that shape the European Union are the interactions with other actors that are shaping them. But why is the European Union feeling such a desire for security at this moment? What has changed in the way Europeans picture their security positions? Trine Flockhart has written an academic study on contemporary security policies and why she believes there is a crisis in the liberal international order. In her article, she starts by acknowledging that it is puzzling why the always thought to be resilient liberal international order is starting to see its walls crack. Because for a long it was viewed that the liberal international order was very resilient as it has global appeal, and deeply embedded practices and because over the past two centuries it has displayed a remarkable ability to adapt and reform in response to crises and adversity (Flockhart, 2020). From a social constructivist perspective, it looks like events have started to shape European security policies in a way that deter it from previous decades. And with a growing concern that the liberal international order is in crisis and its resilience is in doubt (Jervis, 2018), it is understandable that the agency in Europe is starting to feel the shaken. There is no doubt that with United States stating that the liberal international order is in a crisis it challenges the established narrative about security policies. Are European actors to believe that the liberal international order is to continue and be resilient as it always was or are a change underway?

It is very hard to determine what that change will be and perhaps the liberal international order will prevail as it has done before but the examples that have faced European actors and society it has changed their perception of security. The sense of one's security is called "ontological security" and Trine Flockhart argues that the link between ontological security and the ability of agents to invoke their agency to take reflective action is important in this academic paper it is argued that it is apparent in European security policies. Furthermore, detailing how the crisis in the liberal order appears to influence the ontological security of agents of relevance to the liberal international order (Flockhart, 2020). From a social constructivist perspective, it may look like they need for more security and resilience in European financial institutions comes from a place where the self of European security is being threatened by adverse entities. One fact that comes to mind is the nonphysical and non-tangible aspect of cyber-attacks that are now threatening the fundamentals of our society in a way that is not seen before. As before attacks on our sense of security came from physical aspects, examples of this range from terrorist attacks to natural disasters. But today cyber-attacks are threatening our financial institutions and because of financial institutions' central role in monetary services, it threatens our infrastructure and lively hood.

The social constructivist perspective regarding the need for cyber resilience in financial institutions is apparent in the way the European Union creates a picture of the threat picture. The European Union has for example established a "Cybersecurity Strategy Plan" that aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies. The plan is described as a tool to allow more digital security for the European citizen. This is done by boosting the security of essential services and "all connected things" (European Commission, 2020b). Furthermore, by strengthening Europe's ability to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace. The cybersecurity strategy also comes with a reason why all of this is important "everyone should be able to safely live their digital lives". This description of digital safety is not something that our society has laid much thought into before. But it paints a picture that the European
Union believes there is a need for cyber security to protect our "digital lives" (European Commission, 2020b). Perhaps it is trying to somehow materialize and distinguish our physical lives from our digital ones to sort of create a sense of security. However, it shows that the European Union believes there is a need for cyber resilience. Furthermore, the European Union have also laid

out three pillars to support and shape Europe's digital future. First, they will provide "Technology that works for the people", meaning that they will invest in digital skills that can protect people from cyber threats. Furthermore, create a "A fair and competitive digital economy" it could show that the European Union is creating a picture that differs from the aggressive nature of the Chinese expansionist strategy. Now that it cannot rely solely on the tools that a liberal international world order would provide now the European Union is advocating for its sense of responsibility, fair competition, and a vibrant community of innovative and fast-growing start-ups and small businesses to access finance and to expand (European Commission, 2020d). It can be argued that the European Union is following the threat picture established by the United States and therefore they also feel the need to push back against outside influence in the sphere of cyber. Furthermore, the European Union has also felt the decline in the liberal world order and the influence it has had on security. Together with the United States, the European Union is painting a picture in which security and cyber resilience is important for their sense of security.

Weaponized interdependence is a challenge for European security and the implications for this are in terms of cyber resilience and financial institutions a large because of the decline in the liberal world order. But from a social constructivist view what is shaping the European idea of security? In social constructivism, it is important to remember that a large emphasis is on interactions as shapers of reality. An example that has been highlighted earlier was the SolarWinds incident and which showcased the importance of securitization of all entities in the supply chain when it comes to financial institutions. When it comes to weaponized interdependence European actors can look at how the United States has treated Iran, perhaps as far as just after World War 2, to see how interdependencies can have a large impact on security. But that should not be efficient enough to create that sense of unease because the United States is an ally to the European countries. Furthermore, it may be that the European Union has followed the Chinese state and its methods over the past 30 years. The Chinese state has a decent amount of history in using what Farrell and Newman labeled as the two strategies inside weaponized interdependence, the panopticon- and chokepoint effects. First, if you look at what many European citizens experienced through news outlets just two years ago they saw how the Houston Rockets basketball owner and the National Basketball Association were coerced into apologizing for a tweet that showed support for the pro-democracy movement in Hong Kong. The result of this was that the Chinese Basketball Association and Chinese sponsors rapidly suspended their partnerships with the NBA. For a western basketball team in a democratic country with democratic values, the Chinese government is still able to create a chokepoint effect with coercive power to try and force them into firing the Houston Rockets owner (Blennerhassett, 2019). From a liberal point of view, this is just plain crazy for the European standard we see ourselves as having the freedom of speech and getting canceled because of a tweet. Just because that country has more than 300 million people playing basketball (Blennerhassett, 2019). This could arguably be one example of how European actors are viewing the situation our world is in. From Farrell and Newman's point of view, it makes sense that Europe is looking at these examples and thinking perhaps our world is not as resilient as we once thought it was. It paints a picture that coercive interdependence is a tool that adverse states are leveraging to their advantage. Given that they are not playing by the same rules as western liberal states. China can use its media and technology industries both state-run and private as a tool of economic retaliation against whomever they deem as enemies. Of Couse it is presumed that China must have some sort of coercive power over them through interdependencies, however, China is trying to gain more and more control through infrastructure deals or information sharing companies (Farrell & Newman, 2021a; Tusikov, 2021).

The liberal order perhaps is in a crisis just as Trine Flockhart argued. It is a challenge for European resilience as Trine argues for perhaps our idea of a "good life" is an entity not so easily pictured anymore (Flockhart, 2020). It is difficult to articulate what that is in a rapidly changing environment and if there is no agreement on it, therefore it is also difficult to identify the appropriate adaptive measures for a situation where resilience is needed. In the past, our picture of the world was much easier to identify in some sense, for example, during the Cold War it could be argued that the picture established from a social constructivist perspective was blacker and whiter in the sense that either you were with the United State or its allies or with the Soviet bloc. Today that is not the same case, now we have many different entities all struggling for power over their neighbors or across the world. And if you buy into weaponized interdependence the way power is used is much more subtle and intelligent. In the past, most challenges to resilience could be easily identified as some kind of specific threat or concrete problem to which there might be a solution (Flockhart, 2020). Now the solution for handling China's growing influence on the cybersphere is something that both the United States, the European Union, and neighboring countries to China are struggling with. It can be argued that in some way globalization and the liberal international order somehow facilitated "the panopticon" and "the chokepoint" effect by pushing for more and more interdependence. Together with a deterioration of relations between the United States and China, the eagerness of the Donald Trump administration to deploy coercion where it could, and contestation over global supply chains in the wake of the COVID-19 pandemic, it surely looks like weaponized interdependence is a tool of the future. But especially economic coercion is a tool that shapes the way European actors see themselves and how they view their security and resilience challenges (Farrell & Newman, 2021a).

6.3 Discussion of The bank interview, weaponized interdependence, and the social constructive perspective

For the last part of the analysis, an interview has been undertaken to give a better insight into how a real financial institution sees, uses, and understands cyber resilience. The interviewee, is a Chief Information Security Officer. He has been working with security for the past 7 years or so and has been at bank for approximately 2 years dealing with their cyber security. The bank bank is a medium-sized bank that deals with cyber security measures in its daily operations, and they are actively looking into DORA both in terms of compliance but also how the cyber security measure is incorporated into their cyber security management.

The first part of the discussion will talk about the cyber security measures that The bank is dealing with in terms of weaponized interdependence. Weaponized interdependence is from The bank's perspective of greater risk than ever and if you first take a look at the global political picture banks are under more and more pressure from adverse states. CISO'en is arguing for a risk picture that is characterized by greater and greater risk than ever before. He says that "because of all the stuff going in Ukraine with Russia. We have some major risk scenarios that we work within The bank and the sector" (Appendix A, p. 1 (01:39)). CISO'en's risk picture aligns itself with the picture established by the European Union, which states that Russia's actions and "The use of force and coercion to change borders has no place in the 21st century. Tensions and conflict should be resolved exclusively through dialogue and diplomacy" (European Council conclusions, 2022). Instead, this details an enhanced threat picture for critical infrastructure and other entities especially those connected to cyberspace. This is what CISO'en means when he describes a growing risk picture. Furthermore, The bank works on these threats through multiple threat scenarios one being a compromised sub-supplier, another one being a scenario where it is not state-sponsored, and one where it is. They also work with a scenario that takes departure in Russia, so it sounds like The bank has already been through a scenario like the one we are facing now. They also use a scenario that takes its departure in the United States where the government in some forms has comprised a sub-supplier by putting their software into it (Appendix A, p. 1 (01:39)). As CISO'en states it is apparent that The bank is taking different scenarios into account that base itself on weaponized interdependence in some form or another. The bank knows that they would want to secure themselves against adverse states taking advantage of for example their sub-suppliers, in that way they avoid security issues such as the panopticon and chokepoint effect (Farrell & Newman, 2021a). From that point of view, it is defiantly an argument for weaponized interdependence and that it is a security risk and challenges that financial institutions deal with.

Another important characteristic of weaponized interdependence is the issue of centralization of hubs. When asked about it CISO'en answered that it is the main headache of the sector. He stated that "Well, basically it is really the main headache is that what is going on in the sector and other sectors is that more banks are consolidating. Meaning we have bigger entities and before where we had risk spread out in more entities now the sector is more consolidating." (Appendix A, p. 3 (13:26)). CISO'en believes this could mean two things, first that because of the bigger entities the risk picture is less spread out and more manageable. On the other side, the risk picture is getting better and perhaps cheaper for financial institutions to manage. However, perhaps it is also letting criminals in, as they now only must get into one entity instead of having to deal with multiple this could potentially lead to tougher access for hackers. The concept of weaponized interdependence means that centralization affects several dimensions. On one side Farrell and Newman argued that centralization in which central nodes have access to more information may generate a higher amount of security based upon better access to information in the network. But the downside to this is as Farrell and Newman argue that the asymmetric networks that make up much of the structure of the globalized world were not constructed as tools of statecraft. Moreover, they are typically reflected in monopolies or semi-monopolies which focus more on returns rather than security structures. And building more and more centralized networks inadvertently provides adverse actors with the possibility of utilizing their power over the network, whether it be through coercive tools or direct attacks the networks are in some ways more vulnerable than before (Farrell & Newman, 2021a). And as CISO'en mentions this is all based upon how well the setup is and he gives the example of Swift, the global provider of secure financial messaging services, "for example with Swift if you have a good governance around them testing and having people mitigating those things that you find and having good procedures" (Appendix A, p. 5 (21:25)). The idea behind consolidating many financial entities into one is as CISO'en describes it as "… basically you consolidate risk, but you get this operational advantage of having one big entity you can lower the cost of operating" (Appendix A, p. 4 (18:33)). And as for financial institutions, the risks that come with centralization can be mitigated with the right protocols. He states that "there is a lot of good measure to reduce the risk enough that it is okay to consolidate those kinds of things. Also, the society have a good advantage with those kinds of things. It is really a trade of functionality with cost and security. But with the right measures and the right approach, for example DevSecOps. Then it is not necessary a problem" (Appendix A, p. 5 (20:01)). Furthermore, one solution for combatting centralization and issue that persist with it is to make sure that the product being used inside the networks are well produced and tested thoroughly because adverse states will take advantage of the panopticon and chokepoints effects that come with it.

A big vulnerability that CISO'en mentions several times in the interview is the problematic situation surrounding supply chains which is a security challenge for financial institutions. Several examples of this have already been highlighted such as the SolarWinds incident. As just mentioned The bank is even using risk scenarios that involve the United States and their actions towards subvendors which could mean it is a serious threat that might not even come from adverse states in the first place. For financial institutions, the challenge with the supply chains is that they are most vulnerable to both coercive power and direct cyber-attacks. For many years, the idea of cyber security was to "prevent and protect" and today we know that there is more to cyber security than that.

Especially because a financial institution like The bank they have a good eye on its threat security situation. But the sub-vendors they are using such as JN data, who may be supplying The bank with services that interact with their network, may not have the same security standards or tools to avoid attacks. CISO'en's view on this is that The bank or other financial institutions must have their perimeters under control and thereafter advocate for more security in the sector so that their subvendors also get to the same standard of security (Appendix A, p. 9 (37:58)). On the other hand, the European Union is also trying to combat the growing issue of supply chain security mitigation. However, they are also looking at how to prevent adverse states from infiltrating sub-vendors in the financial or other critical sectors so that they are not able to use coercive means to impact our society in negative ways. The European Union stated at the outbreak of the coronavirus pandemic in 2020, a set of guidelines to "protect critical European assets and technology in current crisis". The aim was to "ensure a strong EU-wide approach to foreign investment screening in a time of public health crisis and related economic vulnerability. The aim is to preserve EU companies and critical assets, notably in areas such as health, medical research, biotechnology, and infrastructures that are essential for our security and public order, without undermining the EU's general openness to foreign investment" (European Commission, 2020a). The vulnerability that CISO'en talks about in his statements further correlates with the notion of the European Commission, they are also aware of the dangers that threaten the supply chain in different sectors. Other scholars also highlight the cyber security challenges with the supply chain in today's centralized cyberinfrastructure. And given recent incidents that highlight the resulting economic, political, and social effects it is not surprising that supply chain issues are mentioned in The bank and alike. A reason for this could arguably be the effects of globalization on the interconnectivity of today's digital world that is defining how we do business. It is not only the financial sector that is looking at a clear lack of clarity and gaps in the current knowledge base when it comes to cyber security (Boyes, 2015; Ghadge, Weiß, Caldwell, & Wilding, 2019; Melnyk et al., 2022).

Coercive measures are an important aspect of weaponized interdependence and as Newman and Farrell put it there can both be a panopticon effect and a chokepoint effect (Farrell & Newman, 2021a). Swift is a financial tool that allows the United States and its allies to decide which financial institutions or countries are allowed to use its services. Therefore, they can set up a chokepoint effect for those states that are disallowed the service. The United States and its allies used this to great effect on Russia just when the interview was held and therefore it was apparent to ask CISO'en what he thought about the United States having such tools available. And when asked if "Do you think it is an issue that a country like the United States has more power over a financial tool such as swift?" CISO'en said laughingly that:

> "… Basically, they just did haha. So, yea I think that is the short answer. Yea you know it is also triggers something else it makes the outside world, which is maybe not entangled into swift, makes them aware that hey we are vulnerable if they want to use it against us. Also, you see what is happening now, is that Russia and China are talking about making something similar and yea this is what you get out of it. They did use it and it has a purpose. It triggers some reaction so maybe it is only a onetime thing maybe two I do not know." (Appendix 1, p. 5 (21:25))

The funny element in this is how we are seeing these effects and tools described by Newman and Farrell unfold right before our eyes. The idea and impact behind an action like that is not a new one, however, in a way it surprises CISO'en that it happened and what it did to Russia, however, he might not have believed that there would ever be a situation that would allow such a sanction

against another country. Swift is essential for financial institutions today, however, CISO'en does take it kind of lightly as he suggests that it might only be a one-time tool in the sense that now Russia and
China might be motivated to develop their version of swift to escape the chokepoint effects of it (Handwerker, 2022; Tan, 2022). It could be a possibility as we have seen the two actors go towards more cooperation in the past decade (Malle, 2017).

The next part of the discussion focuses on cyber resilience in financial institutions while also taking into consideration the social constructivist aspects of the The bank interview. The first question in the interview was a simple one that revolved around what CISO'en saw, from a social constructivist perspective it is a safe way of understanding how CISO'en sees cyber resilience and to see if it differs from the textbook example. Cyber resilience is a new idea area in cyber security and there is not a common description of it that all prevail, however, different variations come up and the same goes for CISO'en. He says that cyber resilience is:" it is entities capability to withstand some risk that may occur," furthermore, stating that "Basically, it is we have a threat, and we have some kind of vulnerability that they want to use to get some kind of financial gain. Could also be political. And well cyber resilience is that you have the correct measures to get the risk profile that you want." (Appendix 1, p. 1, (00:22)). This goes in line with other textbook examples which also view cyber resilience as "the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015).

Moreover, an important question worth asking is how does CISO'en as a person in risk management talk about the threat picture in financial institutions today? When asked about he in general terms perceive the cyber threat against financial institutions, he answered that in Denmark they have four levels to the cyber threat picture. The Danish working forum called FSOR short for financial sector forum for operational robustness makes these four levels and at the current time the level is two out of four named "elevated." From a security perspective that seems higher than it should be and the reason it is not higher than it is, is because there is a need to use harder language if a situation gets critical. Even though the security picture has risen over the last years the level still stays the same. However, the day a critical situation or adverse event occurs the level will be raised, and all financial institutions will know that situation is serious. Moreover, he continues to say that

> "Over a long period of time this has almost been the same. Only with a few bumps in the road, one being SolarWinds in December and then Ukraine during the past few months. But generally, the threat picture is defiantly growing, and we also communicate that to our board of directors and to our top management." (Appendix 1, p. 4 (16:31))

CISO'en is watching a security picture that is growing and growing and the words he uses to describe also seem to indicate that the threat picture is getting worse. He specifically uses the phrase "that they are taking a holistic approach to security measures" (Appendix 1, p. 4 (16:31)). A way to describe that they are looking at the whole picture now instead of looking at cyber security in a shallow way is by using a more "risk-based path which takes its point of departure in the threat picture." (Appendix 1, p. 4 (16:31)).

In the interview, CISO'en was asked how he sees The bank as critical infrastructure. To understand his point of view it seemed logical to understand where he sees The bank. The financial sector has considerately evolved over the last 10 years, specifically, the banks have gotten a new role in society, which began with the introduction of digitalized money laundering. Whereas before the police used to monitor and collect information on people, now because of all the digitization of money the banks are serving in this role. Our society has increasingly become cashless, and this has pushed banks into the role of critical infrastructure as their services become key in running society. So, getting CISO'en's perspective on their role as critical infrastructure seemed like a clever way of utilizing the social constructivist perspective and how he pictures their role. CISO'en says that they are used to being a small bank and it is mostly a cultural thing for them. However, they feel like they are in a good spot utilizing the good relations with other parties, which helps to strengthen their financial security and cyber resilience. He further mentions that in Denmark they are all collaborating to a greater extent and positively mentions that this differs from the United States. The Danish approach is working to a greater extent whereas in America they would never allow this level of cooperation between banks (Appendix 1, p. 6 (26:47)). On the other hand, this is an interesting perspective when you look at cyber resilience. There seems to be a good understanding of how to combat cyber threats in Denmark and it mirrors itself in the way The bank operates internally and with its partners. From a social constructivist perspective, it seems like CISO'en describes a healthy picture of cyber resilience in a way that does not indicate an unhealthy amount of recklessness and defiance of limitations.

The bank is a financial institution that tries to be as cyber resilient as possible. In the interview, CISO’en describes different dimensions of the cyber resilience method and thought. The notion of cyber resilience for financial institutions covers several dimensions as was described in the analysis earlier. However, the challenges with hybrid threats where the perpetrator blends two or more tools to conduct the assault were not a part of the analysis. At first, CISO’en did not understand the notion of hybrid threats, however, after clarifying it, it became clear that it is something upon which they have touched. What he says is that the security team was behind multiple scenarios that for example were a phishing type of hacking, a physical USB inside the bank, and a DMZ server getting hacked (Appendix 1, p. 5 (23:03)). A DMZ Network is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic (Fortinet, 2021). The first type of scenario that he mentions is called phishing, a type of cybersecurity threat that targets users directly through email, text, or direct messages. CISO’en argues that this type of scenario is best managed with awareness training. On one hand, Dupont agrees with the notion that awareness training is suitable to combat phishing fraud. His idea that resilience is networked argues that awareness training is part of an information, trust, and security sharing protocol. That both can occur externally as internal and, therefore, it fits into the notion of cyber resilience training. The bank should and is aware that training staff based on shared metrics from other institutions is an effective way to combat these threats. On the other hand, stopping ordinary employees from phishing threats is impossible fully stop, however, by awareness training institutions can both help and survey what the staff is opening. From Dupont’s dimension of cyber adaptiveness The bank is utilizing the dimension of adaptiveness as CISO’en describes how they can quickly survey the threat and challenges in real-time is coming (Dupont, 2019) (Appendix 1, p. 5 (24:08)). It is a challenge to combat these threats and CISO’en further describes a scenario where a man dressed as

an ISS worker, ISS is a cleaning company. The bank called the scenario the “flower water test” and it included a guy that walked into The bank physically and asked to be granted access to the building because he had to water the plants. The man was not a real employee, however, he gained access to all places inside the building and obviously with the wrong intentions could have caused a lot of damage (Appendix 1, p. 5, (24:08)). To be able to have a sufficient level of cyber resilience evaluating your physical perimeters is also of high value. Today we talk about our cyberinfrastructure but for a bank that is still physical, they must think about their cyber resilience in their physical workplace. Dupont also argues for this when he describes the practiced dimension of cyber resilience. Financial institutions must both know the history of cyberattacks, but they must also practice what may come. If they can do it at a high enough level granted that it is not thorough they would gain an enhanced level of cyber resilience (Dupont, 2019). Lastly, the DMZ server scenario also touches upon Dupont's dimension of adaptiveness and practice.

But what happens at The bank once an adverse event is taking place? CISO'en was quick to answer that question and it shows that The bank is ready and has the allocated resources in place for such an event. He said:

> "… we need assess how bad this is. If it is really bad we go into "beredskab". Into emergency state. We have a plan and when it is those kinds of things we also know what kind of processes that is supported by IT and which one of those which are critical for the whole sector. We have a list on that and depending on what kind of processes are being hit" (Appendix 1, p. 7 (29:21))

Highlighting how they first assess how bad the situation is and if they should go into an emergency state. If that is the case they have an emergency plan ready that entails what kind of processes are supported by IT and which ones are crucial to keeping running for the whole sector. CISO'en continues to mention that The bank is part of a network of financial institutions that are controlled by

Fscert an entity in the "finanstilsyn.." CISO'en says that "They have this sector-wide emergency plan and they some certain steps and how does it trigger." (Appendix 1, p. 7 (29:21)). From a cyber resilience perspective, this aligns itself with cyber resilience thought. Both Dupont and Irene Christine

& Thinyane argue that readiness is essential for cyber resilience. And Dupont's dimension of adaptiveness entails that an organization must be quick to reallocate the needed resources during an adverse event. Furthermore, the financial sector's emergency plan that covers all entities is an important dimension because an increase in resilience network is essential to maintaining an enhanced level of cyber resilience. The increase will allow for enhanced information, trust, and response time (Dupont, 2019; Irene Christine & Thinyane, 2020).

The last part of the discussion touches upon DORA and the perspective CISO'en had on the issue and the challenges associated with it. One major part of DORA is strengthening supply chain management and DORA seeks to bring more cohesion to the industry through more information sharing between organizations. The desired result of this is to 'harden' the industry against threats from the collection of hackers, social engineers, and all manner of potential criminal infiltration into services and supplies. Especially the latter part is a big challenge for financial institutions as it has been shown earlier instances of supply chain mismanaging can lead to adverse events. CISO'en agrees with notions as he states that "I think that this vendor-based security management it's just only now getting the right attention." (Appendix 1, p. 9 (37:58)). But what is the real challenge for financial intuitions, one could argue that it perhaps is because of a lack of regulations and standardization resulting in chokepoints in the supply chain. CISO'en argues that on the side the challenge comes from:

> "…it is because of security and the culture inside those vendors that are bottlenecks in the sector. They need to make a drastic change in their way of thinking. They need to come from a "we are a central providing some service that somebody is purchasing" and that is the way is has been. At some point 3 or 4 years ago, they realized that they need to something more." (Appendix 1, p. 9 (37:58))

CISO'en continues to explain that they not only need to think that they are providing a service, but they should also think of security in their perimeters. That way it may be possible to combat situations such as the SolarWinds incident. Furthermore, CISO'en explains that "So, this is a real struggle and I think that somewhere in the future with this whole setup that we have. Because I think we know about the threat picture, and we know about our risk, and we know about all those things. But we need to be more collaborative about security with our sub-vendors and the other way around" (Appendix 1, p. 9 (37:58)). CISO'en believes that DORA could help to put up regulations that will help to create a better foundation for standardization of supply chain security. On one side that would be an increase in security if they can purposely apply it. And as Dupont argues in his dimension of dynamic resilience, organizations must be able to confront themselves in advance with a variety of risks that vary in severity and frequency. Any entities in the supply chain could be able to make the change and enhance their cyber resilience, however, for the entire supply chain to be resilient there needs to be a high amount of work and knowledge put into it. And at this point, it is not sufficient for only the banks to do that work. One issue in this is that all entities in the supply chain do not share information enough. CISO'en also mentions this "It is not sufficient enough for the banks anymore that they do security over at our sub-vendor and we don't know about what's going on. Because maybe we have some understanding of something they don't have taking into account" (Appendix 1, p. 9 (37:58)). That could arguably serve as a real challenge for European regulators and organizations and perhaps it is not the last time we see an incident like SolarWinds (Dupont, 2019).

Overall CISO'en believes the DORA regulations are here to stay and more regulations are the way forward. But will it work is the question? CISO'en believes that it is more of a vision to have a sector-wide regulation throughout Europe. And perhaps he is right, there are certainly going to be differences in the way Danish financial institutions operate and other European financial institutions. But by looking forward there is a possibility that the vision is the right one. CISO'en says that "I think it would be difficult and I think that perhaps it is more a vision maybe. But defiantly a good vision because I know what benefits we get from having the same picture in the financial sector in Denmark." (Appendix 1, p. 10 (42:09)). From a cyber resilience perspective, there is defiantly progress in the way regulators in the European Union are looking at cyber resilience, for example, information sharing, standardization of security protocols, and supply chain management. Moreover, to look forward to a moment what are the possibilities like. What tools are there that may be able to enhance cyber resilience even more? CISO'en mentions one thing that would arguably enhance trust between financial institutions and other entities. Zero trust is a term in financial services where transactions of information or goods can take place without either of the receptors or senders having any information on what is going through. Security in this sense is more enhanced as there is no possibility of hacking as there is zero knowledge of any authentication or goods being sent. CISO'en thinks that: "Zero trust is a lot of things because zero trust in anything. But you need to have strong authentication measures..." (Appendix 1, p. 3 (9:47). Zero trust also comes with challenges that CISO'en describes as you need to be good at revoking access and credentials. You also need to have data discipline and CISO'en believes that is hard and that you can do all access-based controls or trust-based access to the network (Appendix 1, p. 3 (9:47). A technology that is pushing forward in the last couple of years and months is blockchain. CISO'en knows that blockchain is used for a lot of things and it can be used as a validation tool, in that regard it is a possibility. However, latency might be an issue as banks require exceptionally low latency when they are executing thousands of information a day (Appendix 1, p. 3 (12:10). On the other side, Mylrea and Gourisetti argue that blockchain can optimize supply chains through enhanced cyber security, optimization, and compliance. To be able to confront the growing cyber security risks in supply chain management technology and processes must be improved to better identify monitor, and audit vulnerable cyber security risks. They conclude that blockchain could serve as a valuable tool for enhancing cyber security and resilience, however, with all innovative technology it also comes with its challenges. Overall, there is a need for more zero-trust approaches as it will allow financial institutions to enhance cyber resilience to an even greater extent (Mylrea & Gourisetti, 2018).

The The bank case highlighted how financial institutions look at cyber resilience and the growing threat picture in today's cybersphere. Displaying how The bank is trying to combat cyber resilience threats with risk scenarios and preparing for adverse events through information sharing and DORA regulations. All together the interview serves as a vital part of understanding how cyber resilience is being put into the real world.

7. Conclusion

This academic paper sought to illuminate how a liberal and globalized world order is challenging financial institutions' cyber resilience through weaponized interdependence. Financial institutions' cyber challenges corresponded with the notion of "panopticons" and "chokepoints" effects on global economic networks. To be specific, weaponized interdependence challenges financial institutions through the centralization of cyber "hubs" which allows the direct or coercive effect to take place. International actors such as the United States and China both use coercive power tools to gain leverage over centralized global economic networks. European attitude towards outside adverse powers is mimicking the United States' position. It becomes evident that globalization has transformed the liberal order, by moving the action away from multilateral interstate negotiations and toward networks of private actors. Together with the topography of the economic networks of interdependence that intersects with domestic institutions that, therefore, shape norms to coercive authority.

Before the academic paper explored weaponized interdependence further and the pressure on cyber security it analyzed the importance of enhancing different aspects of cyber resilience and the Digital Operational Resilience Act (DORA). It concluded that Dupont's five dimensions of cyber resilience allow DORA to enhance financial institutions' cyber resilience. DORA enhances dimensions in cyber resilience that allows financial institutions to be more dynamic and networked. On a further note, it becomes apparent in the complex dynamics of cyber resilience that there is room for mistakes when enhancing cyber security in the best way. On the other side, cyber resilience is a complex entity that when practiced in an institution is only as good as the knowledge of the people and the training they get. Furthermore, financial institutions need to try and steer away from an environment where performance and efficiency are considered the supreme method. DORA needs to advocate for the conservation of more generalized resources that can be shifted towards management and like to be applied when an adverse situation unfolds. The challenge in cyber security is to allocate enough resources to cyber resilience beforehand to withstand a cyber-attack. The largest challenge and best description of cyber resilience, at this point, is the increase in uncertainty that characterizes financial institutions and the cyber landscape. And even though financial institutions invest heavily in cyber security measures cybercrime is still on the rise, further fueling the uncertainty and insecurity in the sector.

The academic paper contributed a new perspective on international relations and cyber security by combining the new paradigm of weaponized interdependence and cyber resilience in financial institutions. For financial institutions and cyber resilience, it contributed with findings on DORA and the challenges there are in enhancing cyber resilience. Moreover, with an understanding of Trine Flockhart's opinion on European ontological security, it became apparent that our understanding of security has shifted toward a grey area. It is in line with the ideas of weaponized interdependence and pressure put on the liberal international world order through globalization and interdependencies.

Afterward, the social constructivist analysis of the National Defense Strategy and European cyber resilience created a picture of western ideologies clashing with Chinese and Russian anti-liberal doctrines. European cyber politics are closely tied to the political picture the United States is creating of Chinese and Russian norms and ideas towards changing the liberal and globalized world order. Both the United States and the European Union are heavily invested and challenged by adverse states' aggressive actions toward more coercive power in western countries. The social constructivist analysis paints a picture of how European resilience, however, many pictures of said reality can be created, and therefore it only supports one perspective of European cyber resilience. In another case, it is arguably possible that China is the non-aggressor, and the Western countries are working towards less cooperation because of their fear of Chinese and Russian influence.

The subsequent discussion of the findings from the interview with the Chief Information Security Officer at The bank contributed to a distinct understanding of how Europe and financial institutions like The bank Bank describe and understand cyber resilience. Answering questions such as what are the challenges they face from the current cyber threat picture. Moreover, it showcased how a real-world cyber security manager looks at weaponized interdependence challenges such as supply chain vulnerabilities and cyber-attacks. Picturing a financial institution that is highly aware of its cyber security measures and threat picture both internally but just as importantly the international security picture. From a social constructivist perspective, it served as a highly valuable analytic tool when understanding how cyber resilience is viewed by a financial institution, which in terms of strength for the academic paper is of a high degree.

The prospect for weaponized interdependence, cyber resilience, and financial institutions looks to be an area where the security and threat picture is becoming more and more complex. On one side regulatory actions as DORA are enhancing elements of cyber-resilience for financial institutions in Europe and on the other side the tools for adverse states and hackers are becoming better and better. We have arguably not seen the worst adverse events yet and there is defiantly a high risk for financial institution's both in form of panopticons and chokepoints effects from adverse states looking to use coercive power. But also, from smaller groups looking for financial gain in a growing digitalized society. Altogether our society is turning a corner away from the perfect globalized and liberal world order which were thought to bring piece to all corners of the world. Towards a harsher reality where an ideological struggle between the West and authoritarian dictatorships rule. It is not only for financial institutions that cyber are bringing more challenges all corners of our society will see a degree of change in which we perhaps have never seen before.

8. Bibliography

Adey, P., & CISO'enon, B. (2012). Anticipating emergencies: Technologies of preparedness and the matter of security. *Security dialogue, 43*(2), 99-117. doi:10.1177/0967010612438432

Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of cyber security, 1*(3-4), 202-224. doi:10.1080/23742917.2017.1386483

CISO'enen, K. V. (2019). TDC dropper Huawei og lover 5G-net til hele Danmark i 2020. *Tv2*. Retrieved from https://nyheder.tv2.dk/samfund/2019-03-18-tdc-dropper-huawei-og-lover5g-net-til-hele-danmark-i-2020

Ansell, C., Boin, A., & Keller, A. (2010). Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. *Journal of contingencies and crisis management, 18*(4), 195-207. doi:10.1111/j.1468-5973.2010.00620.x

AP. (2020). US hits UAE-based aviation firms with sanctions over Iran. *The Associated Press*. Retrieved from https://abcnews.go.com/Business/wireStory/us-hits-uae-based-aviationfirms-sanctions-iran-72470286

Banga, G. (2020). What is cyber resilience? Retrieved from https://www.balbix.com/blog/resilience/

BDI. (2019). *Partner and Sysmteic Competitor - How Do We Deal with Chinas State-Controlled Economy?* : Federation of German Industries Retrieved from https://e.issuu.com/embed.html#2902526/66954145

Bertucci, M. E., Hayes, J., & James, P. (2018). *Constructivism reconsidered: past, present, and future*. Ann Arbor, Mich: University of Michigan Press.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In *New contributions in information systems and technologies* (pp. 311-316): Springer.

Blennerhassett, P. (2019, October 18). NBA Boss Adam Silver Says Chinese Government Asked Him to Fire Houston Rockets General Manager Daryl Morey. *South China Morning Post*. Retrieved from www.scmp.com/sport/basketball/article/3033476/adam-silver-said-chinesegovernment-asked-him-fire-houston-rockets.

Bodeau, D. J., Graubart, R., Picciotto, J., & McQuaid, R. (2011). *Cyber resiliency engineering framework*. Retrieved from

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *International Monetary Fund*. Retrieved from https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-FinancialSector-A-Framework-for-Quantitative-Assessment-45924

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review, 5*(4), 28.

Britannica. *John Maynard Keynes.* Encyclopedia Britannica. Retrieved from https://www.britannica.com/biography/John-Maynard-Keynes

Brook, R. (2016). *How Everything Became War and the Military Became Everything: Tales from the Pentagon*: Simon and Schuster.

Brumfiel, G. (2004). Publishers split over response to US trade embargo ruling. *Nature, 427*(6976), 663-663. doi:10.1038/427663a

Burr, V. (2015). Social Constructionism. In J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)* (pp. 222-227). Oxford: Elsevier.

Capano, D. E. (2021). Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk. Retrieved from https://www.industrialcybersecuritypulse.com/throwbackattack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

CARNEGIE. (2022). Timeline of Cyber Incidents Involving Financial Institutions. Retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Carter, W. (2017). Forces Shaping the Cyber Threat Landscape for Financial Institutions. *SWIFT Institute Research Paper Series*.

Cerulus, L. (2021). Huawei seeks EU court involvement in Swedish ban *Politico*. Retrieved from https://www.politico.eu/article/huawei-sweden-china-5g-court-case-european-union/

Chirinos, C. (2022). Anonymous claims it hacked into Russian TVs and showed the true devastation of Putin's Ukraine invasion. *Fortune*. Retrieved from https://fortune.com/2022/03/07/anonymous-claims-hack-of-russian-tvs-showing-putinsukraine-invasion/

Coalson, R. (2009). Behind The Estonia Cyberattacks. *RadioFreeEurope*. Retrieved from https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html

Davidson, J. L., Jacobson, C., Lyth, A., Dedekorkut-Howes, A., Baldwin, C. L., Ellison, J. C., . . . Smith, T. F. (2016). Interrogating resilience: toward a typology to improve its operationalization. *Ecology and society, 21*(2), 27. doi:10.5751/ES-08450-210227

Davis, A. (2015). Building Cyber-Resilience into Supply Chains. *Technology innovation management review, 5*(4), 19-27. doi:10.22215/timreview/887

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity (Oxford), 5*(1). doi:10.1093/cybsec/tyz013

Encyclopædia. (2020). ARPANET. In: Encyclopædia Britannica Inc.

EU. (2020). *Digital Operational Resilience Act (DORA)*. (52020PC0595). Brussels Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

European Commission. (2020a). Coronavirus: Commission issues guidelines to protect critical European assets and technology in current crisis [Press release]. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_528

European Commission. (2020b). *The Cybersecurity Strategy*. Retrieved from https://digitalstrategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commission. (2020c). *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*. Retrieved from https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52020PC0595

European Commission. (2020d). *Shaping Europe's digital future*. Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shapingeurope-digital-future_en#relatedlinks

European Council conclusions. (2022). EU response to Russia's invasion of Ukraine. Retrieved from https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/

Fact Sheet: 2022 National Defense Strategy. (2022). Retrieved from https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International security, 44*(1), 42-79. doi:10.1162/isec_a_00351

Farrell, H., & Newman, A. L. (2021a). Weaponized Interdependence and Networked Coercion

A Research Agenda. In H. Farrell, A. L. Newman, & D. W. Drezner (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 305-322): Brookings Institution Press.

Farrell, H., & Newman, A. L. (2021b). Weaponized Interdependence

How Global Economic Networks Shape State Coercion. In H. Farrell, A. L. Newman, & D. W. Drezner (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 19-66): Brookings Institution Press.

FBI. (2022). FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea. Retrieved from https://www.fbi.gov/news/press-releases/pressreleases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democraticpeoples-republic-of-korea

Ferrari, E. (2010). No More Rugs, Pistachios, or Caviar; All Iranian Origin Imports Banned. Retrieved from https://web.archive.org/web/20110716000917/http://sanctionlaw.com/2010/08/21/no-morerugs-pistachios-or-caviar-all-iranian-origin-imports-banned/

Fleming, J., & Ledogar, R. J. (2008). Resilience, an Evolving Concept: A Review of Literature Relevant to Aboriginal Research. *Pimatisiwin, 6*(2), 7-23. Retrieved from https://go.exlibris.link/5VRjYxDx

Flockhart, T. (2020). Is this the end? Resilience, ontological security, and the crisis of the liberal international order. *Contemporary security policy, 41*(2), 215-240. doi:10.1080/13523260.2020.1723966

Foreign, C. D. O. (2022). Foreign Secretary announces 65 new Russian sanctions to cut off vital industries fuelling Putin’s war machine [Press release]. Retrieved from https://www.gov.uk/government/news/foreign-secretary-announces-65-new-russiansanctions-to-cut-off-vital-industries-fuelling-putins-war-machine

Fortinet. (2021). DMZ. Retrieved from https://www.fortinet.com/resources/cyberglossary/what-isdmz

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*.

Girardi, A. (2019). INSTEX, A New Channel To Bypass U.S. Sanctions And Trade With Iran. *Forbes*. Retrieved from https://www.forbes.com/sites/annalisagirardi/2019/04/09/instex-anew-channel-to-bypass-u-s-sanctions-and-trade-with-iran/#66f97d24270f

Goodin, R. E., & Tilly, C. (2006). *The Oxford handbook of contextual political analysis* (Vol. 5): Oxford Handbooks.

Hafezi, P. H. P. (2021). U.S. reluctance to lift sanctions main hurdle to reviving 2015 pact, Iran official says. *Reuters*. Retrieved from https://www.reuters.com/world/china/us-reluctancelift-all-sanctions-main-obstacle-reviving-2015-pact-iranian-2021-12-05/

Halliday, J. (2012). Anonymous distances itself from WikiLeaks. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2012/oct/12/anonymous-distances-itself-wikileaks

Handwerker, N. (2022). Can China's SWIFT Alternative Give Russia a Lifeline? . *The Diplomat*. Retrieved from https://thediplomat.com/2022/03/can-chinas-swift-alternative-give-russia-alifeline/

Hayes, A. (2022). Financial Institution (FI). Retrieved from https://www.investopedia.com/terms/f/financialinstitution.asp

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*, 49-60. doi:http://dx.doi.org/10.5038/19440472.4.2.3

Hewitt & Nephew. (2019). How the Iran Hostage crisis shaped the US approach to sanctions. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2019/03/12/how-theiran-hostage-crisis-shaped-the-us-approach-to-sanctions/

Holling, C. S. (1973). Resilience and Stability of Ecological Systems In L. Robin, S. Sörlin, & P. Warde (Eds.), *The Future of Nature* (pp. 245-260). New Haven: Yale University Press.

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics, 4*(1), 1-23. doi:10.1146/annurev.es.04.110173.000245

Hyland, K., Paltridge, B., & Wong, L. L. C. (2021). *The Bloomsbury handbook of discourse analysis* (Second ed.). London;New York;: Bloomsbury Academic.

IBM. (2021). *Cyber Resilient Organization Study 2021*. Retrieved from https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

Irene Christine, D., & Thinyane, M. (2020, 2020). *Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries*.

Irish, J., & Alkousaa, R. (2019). Skirting U.S. sanctions, Europeans open new trade channel to Iran. *Reuters*. Retrieved from https://www.reuters.com/article/us-iran-usa-sanctions-eu/europeanpowers-launch-mechanism-for-trade-with-iran-idUSKCN1PP0K3

Jervis, R., Gavin, F. J., Rovner, J., Labrosse, D. N., & Fujii, G. (2018). *Chaos in the Liberal Order*

The Trump Presidency and International Politics in the Twenty-First Century: Columbia University Press.

Jibilian, I. C., Katie. (2021). The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. *Business Insider*. Retrieved from https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cybersecurity-2020-12?r=US&IR=T

Jung, H. (2019). The Evolution of Social Constructivism in Political Science: Past to Present. *SAGE open, 9*(1), 215824401983270. doi:10.1177/2158244019832703

Katzman, K. (2022). *Iran Sanctions*. Retrieved from http://www.fas.org/sgp/crs/mideast/RS20871.pdf

Keane, S. (2021). Huawei ban timeline: Detained CFO makes deal with US Justice Department. *Cnet*. Retrieved from https://www.cnet.com/news/privacy/huawei-ban-timeline-detainedcfo-makes-deal-with-us-justice-department/

Keynes, J. M., & Cox, M. (2019). *The Economic Consequences of the Peace: With a New Introduction by Michael Cox*. Cham: Springer International Publishing AG.

Kruger, P. S., & Brauchle, J.-P. (2021). *The European Union, Cybersecurity, and the Financial Sector: A Primer*. Retrieved from https://go.exlibris.link/bbmqzGbv

Krutikhin, M. (2021). Russia's Gazprom: A Case Study in Misused Interdependence. *The Uses and Abuses of Weaponized Interdependence*, 185-200. Retrieved from http://www.jstor.org/stable/10.7864/j.ctv11sn64z.12

Kvale, S. (1998). *InterView: en introduktion til det kvalitative forskningsinterview*. København:

Hans Reitzel.

Kvale, S., & Brinkmann, S. (2015). *Interview: det kvalitative forskningsinterview som håndværk* (3. udgave ed.). København: Hans Reitzels Forlag.

Landman, H. M., Groen, E. L., van Paassen, M. M., Bronkhorst, A. W., & Mulder, M. (2017). Dealing With Unexpected Events on the Flight Deck: A Conceptual Model of Startle and Surprise. *Human factors, 59*(8), 1161-1172. doi:10.1177/0018720817723428

Levs, J. (2012). A summary of sanctions against Iran. *CNN*. Retrieved from https://edition.cnn.com/2012/01/23/world/meast/iran-sanctions-facts/index.html

Linkov, I., Roslycky, L. L., & Trump, B. D. (2019). *Resilience and hybrid threats: security and integrity for the digital world* (Vol. 55). Berlin;Amsterdam, Netherlands;Washington, District of Columbia;: IOS Press.

Linkov, I., & Trump, B. D. (2019). *The Science and Practice of Resilience*. Cham: Springer International Publishing.

Lyngaas, S. (2022). FBI says North Korean hackers stole more than $600 million in cryptocurrency in single hack. Retrieved from https://edition.cnn.com/2022/04/14/politics/fbi-north-koreahackers-crypto/index.html

Malle, S. (2017). Russia and China in the 21st century. Moving towards cooperative behaviour. *Journal of Eurasian Studies, 8*(2), 136-150. doi:10.1016/j.euras.2017.02.003

McGuinness, D. (2018). How a cyber attack transformed Estonia. *BBC*. Retrieved from https://www.bbc.com/news/39655415

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research, 60*(1), 162-183.

Merriam-Webster. (n.d.). Atrophy. *Merriam-Webster*. Retrieved from https://www.merriamwebster.com/dictionary/atrophy

Minami Funakoshi, H. L. a. K. D. (2022). Tracking sanctions against Russia. *Reuters*. Retrieved from https://graphics.reuters.com/UKRAINE-CRISIS/SANCTIONS/byvrjenzmve/

Motamedi, M. (2022). Iran’s economy reveals power and limits of US sanctions. *Al Jazeera*. Retrieved from https://www.aljazeera.com/economy/2022/2/2/irans-economy-revealspower-and-limits-of-us-sanctions

Mylrea, M., & Gourisetti, S. N. G. (2018, 20-23 Aug. 2018). *Blockchain for Supply Chain Cybersecurity, Optimization and Compliance.* Paper presented at the 2018 Resilience Week (RWS).

Nakashima, E. (2017). Israel hacked Kaspersky, then tipped the NSA that its tools had been breached. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-thentipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e2bdd1236be5d_story.html

Oatley, T. (2021). Weaponizing International Financial Interdependence. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 115-130): Brookings Institution Press.

Onuf, N. (2013). *Making Sense, Making Worlds: Constructivism in Social Theory and International Relations*. London: Routledge.

Paloque-Bergès, C., & Schafer, V. (2019). Arpanet (1969-2019). *Internet histories (2017), 3*(1), 1-14. doi:10.1080/24701475.2018.1560921

Perlroth N, S. S. (2017). How Israel caught Russian hackers scouring the world for U.S. secrets. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

Ponemon-Sullivan. (2015). *The Cyber Resilient Organization: Learning to Thrive against Threats*. Retrieved from https://www.ponemon.org/local/upload/file/The%20Cyber%20Resilient%20Enterprise%20Final%2010.pdf

Prescott, K. (2022). West to cut some Russian banks off from Swift. *BBC*. Retrieved from https://www.bbc.com/news/world-60542433

Pricopie, V. (2020). Constructivism. (Generic), 376-378. Retrieved from https://go.exlibris.link/dY8Lh8pN

Raff, A. (2013). From Prevention to Detection: A Paradigm Shift in Enterprise Network Security. *Securityweek*. Retrieved from https://www.securityweek.com/prevention-detectionparadigm-shift-enterprise-network-security

Razin, A., & National Bureau of Economic, R. (2020). *De-globalization: Driven by Global Crises?* (Vol. no. w27929). Cambridge, Mass: National Bureau of Economic Research.

Risien, J. (2000). The C.I.A in Iran: Key Events in the 1953 Coup. *The New York Times*. Retrieved from https://archive.nytimes.com/www.nytimes.com/library/world/mideast/041600iran-ciaindex.html

Roth, A. (2022, 23 March). 'We're going back to a USSR': long queues return for Russian shoppers as sanctions bite. *The Guardian*. Retrieved from https://www.theguardian.com/world/2022/mar/23/were-going-back-to-a-ussr-long-queuesreturn-for-russian-shoppers-as-sanctions-bite

Segal, A. (2021). Huawei, 5G, and Weaponized Interdependence. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 149-166): Brookings Institution Press.

Stecklow, S. (2020). Exclusive: Newly obtained documents show Huawei role in shipping prohibited U.S. gear to Iran. *Reuters*. Retrieved from https://www.reuters.com/article/ushuawei-iran-sanctions-exclusive-idUSKBN20P1VA

Summary of the National Defense Strategy. (2018). Retrieved from https://www.dod.defense.gov/Portals/1/Documents/Pubs/2018-National-Defense-StrategySummary.pdf

Sutton, D. (2018). *Business continuity in a cyber world: surviving cyberattacks* (First ed.). New York, New York (222 East 46th Street, New York, NY 10017): Business Expert Press.

Tan, H. (2022). China and Russia are working on homegrown alternatives to the SWIFT payment system. Here's what they would mean for the US dollar. *Business Insider*. Retrieved from https://www.businessinsider.com/china-russia-alternative-swift-payment-cips-spfs-yuanruble-dollar-2022-4?r=US&IR=T

The Directorate-General for Internal Market, I., Entrepreneurship and SME. (2018). *EU – China cooperation*. Retrieved from https://ec.europa.eu/growth/industry/internationalactivities/cooperation-governments/eu-china-cooperation_en

Tidy, J. (2022). Anonymous: How hackers are trying to undermine Putin. *BBC*. Retrieved from https://www.bbc.com/news/technology-60784526

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Retrieved from https://www.theguardian.com/world/2007/may/17/topstories3.russia

Tusikov, N. (2021). Internet Platforms Weaponizing Choke Points. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 133-148): Brookings Institution Press.

Vallance, C. (2022). UK blames Russia for satellite internet hack at start of war. *BBC*. Retrieved from https://www.bbc.com/news/technology-61396331

Weiwei, A. (2022). Ai Weiwei on the new Silk Road: 'This is China's counterattack in a global game of chess'. *The Guardian*. Retrieved from https://www.theguardian.com/world/2022/mar/19/ai-weiwei-new-silk-road-chinese-powergrab

Woo & Viswanatha. (2018). Huawei Under Criminal Investigation Over Iran Sanctions Retrieved from https://www.wsj.com/articles/huawei-under-criminal-investigation-over-iransanctions-1524663728

Young, I. (2021). China's ambassador warns Canada against Huawei 5G ban, saying 'Meng Wanzhou incident' should be a lesson *South China Morning Post*. Retrieved from https://www.scmp.com/news/china/diplomacy/article/3158831/chinas-ambassador-warnscanada-against-huawei-5g-ban-saying

Appendix:

App. 1: "Interview transcription"

App. 2: "Interview guide"

Frontpage retrieved non-copyright at: https://unsplash.com/photos/EUsVwEOsblE