universität wien

Master Thesis

Titel der Master Thesis / Title of the Master's Thesis

"Assertive vs. Defensive Actors in Cyberspace? An IR and Legal Comparison Between the United States and European Union's Cybersecurity Strategies "

verfasst von / submitted by

Lara Siebrecht

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Advanced International Studies (M.A.I.S.)

Wien 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt Postgraduate programme code as it appears on the student record sheet:	A 992 940
Universitätslehrgang lt. Studienblatt Postgraduate programme as it appears on the student record sheet:	Internationale Studien / International Studies
Betreut von / Supervisor:	Prof. Dr. Arthur R. Rachwald

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

Acknowledgements

I would like to take this opportunity to thank everyone who supported me while pursuing this degree and master's thesis.

To my thesis supervisor, Dr Prof. Arthur Rachwald, thank you for your professional and personal advice that I will always treasure. I also thank all the other great professors at the Diplomatic Academy who have taught me more than I could have ever hoped for in these past two years.

To my peers who have become great friends: Thank you for our dear friendships and for always encouraging me when I needed it the most. The DA truly is a special place due to the diverse and amazing people who will forever leave an impact on me.

Finally, I would like to thank my parents, my sister, and my boyfriend for always believing in me no matter what. I could not have done this without your constant support. This one's for you.

Table of Contents

List of Acronyms

CER Directive	Critical Entities Resilience Directive
DoD	Department of Defence
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
NIS Directive	Network and Information Security Directive
U.S.	United States
USCYBERCOM	United States Cyber Command

"On my honour as a student of the Diplomatische Akademie Wien, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it."
-Lara Siebrecht

Abstract

This thesis identifies whether the United States, an assertive/proactive international actor necessarily has more advantages in securing cyberspace than the European Union, a rather defensive/reactive international actor. The thesis approaches this research question from an international relations and legal perspective while drawing data and information from legislation, policies and conducting interviews. It recognises that cyberspace and cybersecurity do not fit in one single IR theory, but also argues that classical, offensive, and defensive realism can be adopted for the needs of this study. After an extensive comparison and analysis between the United States and European Union's cybersecurity strategies, policies and legislation, the thesis concludes that the United States has some advantages in cyberspace and cybersecurity due to its assertive international character. However, these advantages are also limited since both the U.S. and the EU struggle with similar challenges when forming cybersecurity policies and legislation.

Abstrakt

Die Masterarbeit befasst sich mit der Frage, ob ein eher durchsetzungsfähiger/proaktiver Staat, wie die USA, grundsätzlich mehr Vorteile in der Cybersicherheit hat als die EU. Die Frage wird gestellt, da die EU als eher defensiver/reaktiver internationaler Akteur eingeschätzt wird. Nach einem ausführlichen Vergleich und einer Analyse der relevanten Gesetzgebungen, Strategien, Politik und geführten Interviews kommt die Arbeit zu folgendem Fazit: Durch ihren durchsetzungsfähigen/proaktiven Charakter hat die USA zwar einige Vorteile in der Cybersicherheit, jedoch sind diese limitiert. Die EU und die USA beschäftigen sich in ihrer Politik oftmals mit den gleichen Hürden, insbesondere in Bezug auf die Cybersicherheit.

1. Introduction

Cyber is a growing domain that is becoming ever more relevant and cannot be ignored in international relations and international law. Because we are shifting toward an increasingly internet-dominated world, it is obvious that policies need to be formed in this realm, not just from a domestic point of view, but also from an international one. However, due to the vast and new nature of cyber, politicians, experts and lawyers struggle to keep up with shaping effective cybersecurity strategies. Forming cybersecurity strategies is especially challenging since non-state actors are gaining more power in this realm and the source of a cyberattack often remains difficult to identify. Nevertheless, effective policies around cyber are currently essential since cyberattacks are increasing and pose significant threats to states, individuals, the public, and the private sector. Up until today, we have not witnessed the full potential of a cyberwar. But, with international conflict increasing in the twenty-first century, the unknown outcome of a full cyberwar could be revealed in the near future. In this sense, international actors such as the United States and the European Union must be prepared to interact on a strategic level in cyberspace. Recently, dominant states, such as China and Russia have been attributed as the sources of major cyberattacks, some of which will be analysed in the thesis. The question is whether Western states and international actors, like the United States and the European Union, are fully prepared for cyberattacks if not even for a cyberwar with Russia and China. For successful strategy and execution in cyberspace, an understanding of this space from an international relations point of view is the missing factor that complements the technical understanding of cyberspace. Therefore, with this thesis, I would like to contribute toward the conceptual understanding of cybersecurity not simply from a technical point of view, but through the lens of international relations and law. More specifically, the thesis will provide a comparison between the cybersecurity strategies of the United States and the European Union and will investigate whether a rather assertive state in international relations will necessarily be more successful in cyberspace that a defensive actor. An exact explanation of what is meant by an “assertive” and “defensive” international actor will be provided in the research question.

The reason why I chose to pursue this thesis topic is partially due to the seminar I took the previous year on U.S. cybersecurity policy with Dr. Professor Harknett from the University of Cincinnati. The academic approach and strategy the U.S. has adopted in the field of cybersecurity made me curious as to how the European Union approaches cybersecurity policy and strategy. Why the European Union was selected as a comparison to the United States is perhaps at a first glance not obvious. After all, the United States is a state itself and the European Union is formed by several member states. Why not compare the United States to a single state?

The reason the European Union was chosen lies in the fact that is seen as an international actor itself. The European Union as an entity exists and is recognised in cyberspace. Furthermore, one can say that Europe is the strongest when its member states form a Union. In the sense of power and geography, it is, therefore, appropriate to compare the United States and the European Union. Furthermore, individual states of the European Union, like Estonia, France and Norway might have implemented a stronger cybersecurity strategy than some of their European allies. However, if the European Union could implement strong cybersecurity strategies and policies for the entire Union, this would benefit all member states. Let us say a cyber-attack would hit core European institutions. This would affect all member states, even those which have a strong cybersecurity policy implemented within their own borders. For the reasons mentioned, a cybersecurity comparison between the European Union and the United States is valid.

2. Literature Review

The literature review serves the purpose to analyse and draw conclusions from existing literature on cybersecurity strategy within the European Union and the United States, including the theory that has so far been attributed to cyberspace.

First, the book *Cybersecurity and Cyberwar: What Everyone Needs to Know*, by Allan Friedman and P.W. Singer was considered for not only the literature review, but also for gaining an overall insight into the topic of cyberspace and how it relates to international relations and policy. According to Friedman and Singer, cyberspace can be defined as "the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online."[1] It is an "information environment," compromised "by computers that store data plus the systems and infrastructure that allow it to flow," and is "constantly evolving."[2] The authors provide an informative book that will, later on, assist the thesis in some of its chapters. Something relevant the authors mention in the book is whether offensive or defensive actors in cyberspace have the advantage.[3] In traditional military concepts, the offensive actor would have the best weapons and the stronger willpower which would allow him to win on the battlefield. However, the authors also highlight that the offensive approach, even in a traditional sense also has its disadvantages, such as prompting war and death. Also in cyberspace, "the offense's inherent advantage is not so simple," as cyberattacks "take long periods of planning and intelligence gathering to lay the groundwork" and a "great deal of expertise."[4] As for the defensive side, "the amount of 'ground' that the defender has to protect is almost always growing in the cyber world, and growing exponentially."[5] However, Friedman and Singer explain that the defender is "not so helpless in cybersecurity" as one would think.[6] In fact, the "attackers may have the luxury of choosing the time and place of their attack, but they have to make their way through a 'cyber kill chain' of multiple steps if they actually want to achieve their objectives."[7] Additionally, "a defender can stop the attack at any step."[8] In relation to this, the authors conclude that a very good defense might give an actor superiority in cyberspace. They say that "any steps that raise the capabilities of the defense make life harder on the offense

[1] Allan Friedman and P.W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press, 2014, p.13.
[2] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p.13-14.
[3] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 153.
[4] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 154.
[5] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 154.
[6] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 155.
[7] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 155.
[8] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 155.

and limit the incentives for attacks in the first place."[9] However, the offense should still not be underestimated. These remarks on offense and defense in cyberspace will be considered for the thesis' research question of whether an assertive actor necessarily has more advantages in cyberspace.

From an EU perspective, the articles of Carrapico and Barrinha, Sliwinski, Wang, Anagnostakis, Markopoulo, Papakonstantinou, de Hert and Edegbeme-Beláz were considered. In terms of a cybersecurity timeline in the EU, Edegbeme-Belàz identifies several phases in which the role of the EU in cybersecurity has shifted and explores the various policies that have evolved in these. The author mentions "the beginnings 1985 – 2001," "the facilitating role 2002-2006," "the awakening 2007-mid 2016," and the "repositioning EU in the cyber sector mid2016 – nowadays."[10] This summary provides a helpful and brief overview of what policies have been developed in the European Union in terms of cybersecurity. Also, Wang "discusses the most recent EU cybersecurity legislative movements (2013-2019)," including the EU Cybersecurity Act 2019, which will contribute toward forming a brief overview of cybersecurity policy developments in the European Union.[11] Something that several authors mention about the EU's role in cybersecurity is its rather defensive nature. Carrapico and Barrinha conclude after an analysis of the European Union's vertical and horizontal relations that although cybersecurity is gaining more attention and priority within the EU, the EU is still a rather less assertive security actor, which will back up this thesis' argument on the EU's more defensive, and less assertive role in cybersecurity.[12] Also Sliwinski criticizes the defensive nature of the EU's cybersecurity, explaining that this only gives the EU limited influence in the cybersecurity realm.[13] Examples of this would be a "broad coordination" of "ENISA," the European Union Agency for Cybersecurity, and the intergovernmental character of the EU's Common Foreign and Security Policy.[14] Furthermore, Markopoulou et al.'s definition of a "late response to an already exacerbated and well-known problem"[15] confirms the thesis' categorization of the EU's cybersecurity strategy in Defensive Realism. Speaking of limitations, most articles in this literature review criticize the European Union's member states themselves that limit its

[9] Friedman and Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 155.
[10] Edegbeme-Beláz, Annamária. "The changing role of the EU in cybersecurity." *Legal and strategical aspects of information and cyber security* (2019): 19-26.
[11] Faye F. Wang, "Legislative Developments in Cybersecurity in the EU," *Amicus Curiae: The Journal of the Society for Advanced Legal Studies* 1, no. 2 (2020): 238.
[12] Carrapico and Barrinha, 1267.
[13] Sliwinski, 14.
[14] Sliwinski, 14.
[15] Markopoulou, Papakonstantinou and De Hert, 11.

cybersecurity strategy and policy. Carrapico and Barrinha, for example, mention "resistance from Members states to allow the EU to have more stringent control over their cyber activities," as a limitation of the European Union's cybersecurity.[16] Like Carrapico and Barrinha, Edegbeme-Beláz confirms that EU institutions struggle to coordinate with one another, which limits the EU in executing a successful cybersecurity strategy.[17] Additionally, the author emphasizes the difficulties of "EU and Member state level cooperation on cybersecurity," and the "question whether the Member states are willing to engage."[18] Sliwinski stated in 2014 that the European Union is limited by its "intergovernmental character and the corresponding lack of collective vision on the part of the member states."[19] Another limitation of the European Union's cybersecurity policy can be found in the lack of an exact definition or clarification of cybersecurity and a compulsory and productive way of incorporating cybersecurity within the EU in 2014.[20] Similar to this, Wang points out how the EU has somewhat set up "numerous new creations [...] to work on regulatory developments on cybersecurity issues in the EU," but somehow lack a "logical structure and with clean and non-duplicated functions."[21] Also Markopoulou et al. mention how the NIS Directive and the General Data Protection Regulation do not "acknowledge each other in their respective texts," which displays digital law within the European Union has an indecisive nature and therefore cannot be as assertive, as for example the U.S.[22] Furthermore, Wang displays that the EU's new initiatives on cybersecurity need to be more "carefully thought out in terms of definitions, functions, responsibilities, connections and relationships with one another," and the technical measures of these initiatives need to be more researched.[23] Lastly, the author identifies some "key measures in order to combat cyber threats and attacks and increase cybersecurity," which suggests that the EU is indeed limited in its cybersecurity policy.[24] The question remains whether this is partially due to its defensive character in international relations, but also in cybersecurity itself. Overall, other remarks worth mentioning were found regarding EU literature on cybersecurity policy. What is particularly interesting and what will be acknowledged from this study is how Carrapico and Barrinha define cybersecurity as a realm in which a "lack of transparency" and "accountability" are common.[25] This might additionally limit the European Union as its policy is mainly based on

[16] Carrapico and Barrinha, 1267.
[17] Edegbeme-Beláz, 26.
[18] Edegbeme-Beláz, 28-29.
[19] Sliwinksi, 13.
[20] Sliwinksi, 13-14.
[21] Wang, 247-248.
[22] Markopoulou, Papakonstantinou and De Hert, 9.
[23] Wang, 247.
[24] Wang, 254.
[25] Carrapico and Barrinha, 1268.

"values" and "democratic governance," whereas the United States might find it easier to operate such a space.[26] On another note, Sliwinski mentions that academic literature in cybersecurity is more prominent in the "defense policies of big powers, especially China and the United States," something that has also been identified while conducting this literature review.[27] The notably higher percentage of academia in these countries might suggest that big powers, such as the United States and China, are more assertive, in particular from a strategic standpoint in cyberspace. Finally, the literature does not necessarily compare the United States and the European Union's cybersecurity strategies but rather analyses their relationship in this field, which can also be helpful for finding similarities between the two strategies in the thesis. Anagnostakis displays the strengthening cooperation between the two players in internal security despite political tensions, which is based on similar interests in principles, norms, values, and threat perceptions.[28] The current cyber relationship between the U.S. and the EU is currently displayed by the EU-US "Working Group on Cybersecurity and Cybercrime" and the EU-US "Cyber Dialogue."[29] Something else that is interesting is how Anagnostakis compares Russia and China, the more state-controlled cyber- and security strategies, to those of the U.S. and the EU, which are based on "common principles and norms."[30] So, another question for the thesis might be whether the U.S. and EU cyber policies have more in common than initially expected?

From a U.S. point of view, Richard Harknett already argued in 2003 that it is difficult to categorize cybersecurity in the school of Realism since the "multidimensional" nature of globalization has led to "unattributable disruption and destruction. The author displays "Integrated Security," an approach that recognizes "the interconnectedness of a continuum of security models," and how sole deterrence is not applicable anymore in the twenty-first century due to anonymous and non-state attackers/actors.[31] Due to the internet's "accessibility," "availability," "speed," "affordability," and the possibility of "individual empowerment," Harknett argues that we have shifted away from nuclear deterrence in the information age.[32] Even though the thesis will categorize EU and U.S. cybersecurity strategies in defensive and offensive realism, it will also consider Harknett's argumentation of why Realism cannot solely be the theory used for cyberspace. Apart from theoretical application questions, something that

[26] Carrapico and Barrinha, 1268.
[27] Sliwinksi, 14.
[28] Anagnostakis, 1.
[29] Anagnostakis, 1.
[30] Anagnostakis, 5-6.
[31] Harknett, "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few," 14.
[32] Harknett, "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few," 18-23.

this article displays is how the United States has academically approached the topic of cybersecurity strategy and policy earlier than the European Union. Already in 2003, authors like Harknett questioned the notion of deterrence in cyberspace, something EU scholars have not done. How academic input influences U.S. cybersecurity policy differently than the EU will be further explored in the thesis. Craig and Valeriano, in controversy to Harknett, argue that Realism can be a suitable paradigm "in explaining international cyber politics," even though it also "lacks the ability to explain the dynamics of cyber conflict."[33] The anarchical character of cyberspace, for example, argues for Realism since "the cyber domain lacks effective global institutional governance."[34] Additionally, "Realism can help explain the source of cyber arms racing behaviour as a response to threat in an anarchic world," in which "capabilities are very difficult to distinguish."[35] However, the authors also mention why realism cannot explain cyberspace. For example, non-state actors have, next to states become relevant in cyberspace.[36] This also leads to the fact that "traditional power dynamics," which are reflected in realism, are challenged in cyberspace. Furthermore, "unlike nuclear weapons, cyber weapons do that have the same destructive capacity and so, to have a sufficient deterrent effect," and one cannot always detect the attacker.[37] This paper overall displays the arguments for and against realism in cyberspace, which will help form an argument as to how the European Union resembles defensive realism in its cybersecurity strategy.

Apart from the theoretical point of view, Kenneth Geers explains that the United States "was the first nation to create a military command devoted entirely to cyber war, but since then, all major powers have followed suit."[38] This suggests that the United States treated cyberspace as a primarily military space, in which she proceeded to be ahead of the game from other international actors. This, again, hints toward her assertive character as a state. However, Geers also highlights that it is essential, even for a powerful state such as the United States to deal with cyberspace on an international, rather than national level. Cybersecurity is "'an international problem that requires an international solution,' even while myriad geopolitical rifts are likely to endure for the foreseeable future."[39] Also, in one of his more recent articles, Richard Harknett elaborates on how the United States has recognised the unique nature of

---

[33] Anthony J.S. Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age." *In Realism in Practice*, edited by Davide Orsi, J.R. Avgustin and Max Nurvus, 85-101. Bristol: E-International Relations Publishing, 2018, 85-86.
[34] Anthony J.S. Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," 88.
[35] Anthony J.S. Craig and Brandon Valeriano, 88.
[36] Anthony J.S. Craig and Brandon Valeriano, 90.
[37] Anthony J.S. Craig and Brandon Valeriano, 94.
[38] Kenneth Geers, "Alliance Power for Cybersecurity," Atlantic Council, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Alliance-Power-for-Cybersecurity_Geers.pdf, 6.
[39] Geers, "Alliance Power for Cybersecurity," 2.

cyberspace in the United States Cyber Command. For example, the U.S. acknowledges that "cyber operations have opened a new seam in the distribution of power and can impact relative power without traditional armed aggression"[40] and that non-state actors are capable of "damaging American interests," not just states themselves.[41] The United States has additionally recognised the "interconnected nature of cyberspace" in which "constant contact and shifting terrain […] continually challenges ones' capacity to defend and to maneuver"[42] These are strategic aspects that scholars like Richard Harknett have detected in the realm of cyberspace.[43] It is significant that the U.S. has acknowledged academic findings of cyberspace from the school of international relations and includes them in the United States Cyber Command. The U.S. has come to realise that a "sustained analysis of cyber operations" has become as important as nuclear deterrence.[44] This is a dynamic that has not been clearly detected in the European Union's cybersecurity strategy and again suggests that the EU lags behind the United States in cyberspace and cyber power. Lastly, the statement that "opponents […] will accuse the United States of potentially militarizing cyberspace through this approach"[45] suggests that the U.S. is a more assertive player not only as a state but also as a cybersecurity actor. Harknett, however, justifies the new Cyber Command as "not an offensive doctrine, but a seamless operational approach integrating resilience, defense and contestation of adversary activity."[46] Something else that is important to mention in the literature review is Harknett's and Fischerkeller's understanding of "constructing norms in cyberspace."[47] The authors reflect on how the U.S. has shifted toward a cybersecurity approach that acknowledges that "armed conflict and deterrence strategy in its own is not an effective anchoring approach for ensuring security in this strategic competitive space."[48] The authors see the United States' step toward the adoption of *persistent engagement* in its cybersecurity strategy as an important step "toward regaining U.S. strategic advantage."[49] *Persistent engagement* can be "understood as continuously engaging and contesting adversaries and maneuvering for advantage below the threshold of armed conflict," which is a "fundamental feature of tacit bargaining."[50] Additionally, *persistent engagement* is

[40] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," *Lawfare* (March 2018), 123.
[41] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," 123.
[42] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," 123.
[43] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," 123.
[44] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," 126.
[45] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," 124.
[46] Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it Matters," 124.
[47] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*," Lawfare* (November 2018), 117.
[48] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*," Lawfare* (November 2018), 117.
[49] Michael P. Fischerkeller and Richard J. Harknett, 120.
[50] Michael P. Fischerkeller and Richard J. Harknett, 120.

an approach that "recognizes that cyberspace's structural feature of interconnectedness" and "constant contact."[51] The authors claim that states must adopt this strategy to be "more secure in cyberspace" and to "position themselves to enhance their national power relative to others."[52] Furthermore, *Tacit bargaining* means abandoning "traditional approaches" of bargaining in cyberspace, and rather coming to "informal agreements" and "patterns," which leads to more "clarity" and "predictability."[53] Reading literature on cyberspace strategy from an EU perspective, I have not come across the notion of *persistent engagement* or *tacit bargaining*. One could argue that the United States' more assertive character as a state has pushed her to recognize and understand cyberspace as a competitive space earlier than the European Union. The question remains if this approach gives the U.S. more strategic advantages in cybersecurity strategy and execution than the European Union.

Overall, the existing literature currently suggests how the EU is a less assertive security actor[54] and how the nature of EU cybersecurity policy is rather defensive.[55] Additionally, several findings exist on how the European Union is limited in its cybersecurity[56] and the diplomatic relationship between the EU and the U.S. in cybersecurity.[57] While conducting the literature review, noticeable research gaps were found, too. For example, an actual comparison between the United States and the European Union's cybersecurity policies from an international relations point of view was not found, which means that this thesis will have a novel approach. Furthermore, the European Union's literature on cybersecurity policy is rather based on its timeline, what has legally been passed so far and the gaps and limitations of the EU's cybersecurity policies themselves. U.S. literature, on the other hand, additionally portrays international relations theory and the notion of deterrence in cyberspace, something that could not be found in the EU literature. This suggests that the United States has dealt with questions of cybersecurity strategy longer and in more depth than the European Union and therefore could hint toward the country's more assertive character as an international actor.

---

[51] Michael P. Fischerkeller and Richard J. Harknett, 117.
[52] Michael P. Fischerkeller and Richard J. Harknett, 117.
[53] Michael P. Fischerkeller and Richard J. Harknett, 118.
[54] Helena Carrapico and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?" *Journal of Common Market Studies* 55, no. 6 (2017): 1254-1272.
[55] Krzysztof Feliks Sliwinksi, "Moving beyond the European Union's Weakness as a Cybersecurity Agent," *Contemporary Security Policy* (September 2014): 1-19.
[56] Sliwinksi, Wang, Markopoulo et al., Edegbeme-Beláz.
[57] Dimitrios Anagnostakis, "The European Union-United States cybersecurity relationship: a transatlantic cooperation," *Journal of Cyber Policy* 6, no.2, (April 2021): 1-19.

3. Research Question

The thesis mainly focuses on EU policy and strategy that has evolved around cybersecurity and later makes comparisons to the United States' approach on this. More specifically, the EU's evolving cyber strategy seems to be at a first glance less assertive, which is why it will be compared to the cybersecurity strategy of the United States, a global actor who has up until today proven to be more assertive in international politics than the European Union. What is meant by an "assertive" international actor when referring to the United States is a state that has been proactive in international relations from a strategic and military point of view in the twentieth and twenty-first century. The European Union, on the other hand, is referred to as a "defensive" international actor since it is rather reactive than proactive in international relations. The United States has positioned itself as the Western hegemon, whereas the European Union rather follows and agrees with the democratic principles of the United States. **In this sense, the thesis questions whether the United States' more assertive international character necessarily gives the country more advantages in cybersecurity than a rather defensive actor, the European Union?** The thesis tackles the research question with a multidisciplinary approach. On the one hand, the discipline of international relations will be used as a theoretical framework for both the United States and the European Union's cybersecurity strategies. On the other hand, the discipline of international law approaches the relevant cybersecurity legislation of both actors.

4. Theory

Cyberspace is a unique and new domain in which a theoretical framework is hard to come by. Therefore, the thesis adopts existing theories for the needs of this study. The thesis argues that classical realism is the most fitting general paradigm for cyberspace. Realism is an international relations theory that claims that "states live in a context of anarchy," in which "rational decision-making leads to the pursuit of the national interest" and to "survive in a competitive environment."[58] There are many arguments for why cybersecurity can be linked to this theory. Craig and Valeriano for example display that cyberspace's "anarchical nature and lack of institutional governance where states fear one another and develop their capabilities in response," as well as "questions of cyber power" suggest the theory of realism.[59] Furthermore, "the offense-defense balance," "uncertainty" and "prudent behaviour" in cyber argue for the paradigm of realism.[60] Overall, the anarchic character of cyberspace itself is a major reason why realism must be considered as a theoretical framework for this study. Furthermore, some of the arguments of classical realist Hans Morgenthau in "Politics Among Nations: The Struggle for Power and Peace," can be linked to cyberspace. First, Morgenthau argues that "political realism believes that politics, like society in general is governed by objective laws that have their roots in human nature."[61] In cyberspace, objective laws that govern this anarchic realm, also are derived from human nature since humans created and control cyberspace. Second, Morgenthau claims that "the concept of interest is defined by power"[62] In cyberspace, we can observe a similar theme: The more power an actor has in cyberspace, whether this is achieved by successful hacking skills, or other means, the more this actor can follow his/her interests. Furthermore, classical "realism assumes that its key concept of interest defined as power is an objective category which is universally valid."[63] This is also true for cyberspace. In cyberspace, interests of power are valid in a universal sense; It does not depend on the place and time. Cyberspace is an anarchical, universal space where norms do not differ from actor to actor. Morgenthau additionally says that "Political Realism is aware of the moral significance of political action."[64] In cyberspace, actors are likewise aware of their actions and of the morals each of their actions entail. This also means that realism in cyberspace refuses "to identify the

---

[58] Sandrina Antunes and Isabel Camisão,"Introducing International Relations Theory," E-International Relations , February 27, 2018, https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/.
[59] Anthony J.S. Craig and Brandon Valeriano, 94-95.
[60] Anthony J.S. Craig and Brandon Valeriano, 95.
[61] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 5th ed., revised, (New York: Alfred A. Knopf, 1978), https://www.mtholyoke.edu/acad/intrel/morg6.htm.
[62] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace.*
[63] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace.*
[64] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace.*

moral aspirations of a particular nation with the moral laws that govern the universe."[65] As displayed in Hans Morgenthau's arguments of classical realism, many points of the international relations theory generally fit into cyberspace.

When it comes more specifically to the European Union and the United States, the thesis adopts the theoretical framework of structural realism. As for the European Union, the thesis argues that cybersecurity and cyber strategy can be categorized as defensive realism. In defensive realism, "anarchy encourages states to adopt defensive, moderate, and restrained strategies."[66] The European Union seems to fall behind other powerful states in issues of cybersecurity and the EU's attempt at new legislation and strategy suggests a defensive/reactive response toward anarchy in cyberspace. As for the United States, the thesis assumes that the United States' cybersecurity strategy leans more toward offensive realism due to its assertive/proactive character as a state. Offensive realism suggests that "anarchy compels states to maximize influence, to compete for power in a never-ending struggle for hegemony."[67] Something that should be considered at the same time is that the U.S. and EU share "common principles and norms" in their strategies and have also built a working group.[68] This also hints toward a neoclassical realist framework in which states tend to balance their power with other actors. The U.S. and EU seem to, simultaneously to their own cybersecurity strategies, balance their power against enemies in the anarchic realm of cyberspace.

Lastly, it is important to mention that the U.S. has shifted toward acknowledging the need for "persistent engagement" and "tacit bargaining" in its cybersecurity strategy.[69] As explained in the literature review, *persistent engagement* can be "understood as continuously engaging and contesting adversaries and maneuvering for advantage below the threshold of armed conflict," which is a "fundamental feature of tacit bargaining."[70] *Persistent engagement* also "recognizes that cyberspace's structural feature of interconnectedness" and "constant contact."[71] *Tacit bargaining,* on the other hand, means the abandonment of "traditional approaches" of bargaining in cyberspace, and shaping "informal agreements" and "patterns," which leads to more "clarity" and "predictability."[72] *Persistent engagement* and *tacit bargaining* are means

---

[65] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace.*
[66] Steven E. Lobell, "Structural Realism/Offensive and Defensive Realism," *International Studies: International Study Association and Oxford University Press,* (December, 2017): https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304, 10.
[67] Steven E. Lobell, "Structural Realism/Offensive and Defensive Realism," 10.
[68] Anagnostakis, "The European Union-United States cybersecurity relationship: a transatlantic cooperation," 5-6.
[69] Michael P. Fischerkeller and Richard J. Harknett, 120.
[70] Michael P. Fischerkeller and Richard J. Harknett, 120.
[71] Michael P. Fischerkeller and Richard J. Harknett, 117.
[72] Michael P. Fischerkeller and Richard J. Harknett, 118.

that have not been identified in the EU cybersecurity strategy so far. This hints toward the European Union's rather reactive/defensive character in cyberspace. Therefore, defensive realism can be adopted for the EU's cybersecurity strategy. The fact that the United States, on the other hand, proactively uses means of *persistent engagement* and *tacit bargaining* in its cybersecurity strategy proves that the country is an assertive character in cyberspace. As such, offensive realism can be adopted for the United States' cybersecurity strategy.

In terms of legal theory, legal positivism is used in the thesis to analyse the cybersecurity policies and strategies of the European Union and the United States. According to Marmor, "legal positivism is best understood as a descriptive, morally neural, theory about the nature of law."[73] Furthermore, "the theory need not take a stance on any particular moral or political issues, nor is it committed to any moral or political evaluations."[74] More specifically, legal positivism argues that "the law is essentially a means," and "instrument" as Hans Kelsen once said.[75] The law is "a matter of social facts" and it "depends on the social rules that prevail in the relevant society".[76] A part of legal positivism that has been criticised in many ways is the *separation thesis*.[77] This is because legal positivism denies a "possible dependence of law on moral considerations."[78] Even though this theory of law has been controversial and criticised, the thesis takes the approach of legal positivism while analysing legal texts since the thesis does not aim to identify whether U.S. or EU cybersecurity law is moral or not, but rather its nature.

[73] Andrei Marmor, "Legal Positivism: Still Descriptive and Morally Neutral," *Oxford Journal of Legal Studies,* vol. 26, No. 4 (2006), 683.
[74] Andrei Marmor, "Legal Positivism: Still Descriptive and Morally Neutral," 683.
[75] Marmor, 685.
[76] Marmor, 686.
[77] Marmor, 686.
[78] Marmor, 686.

5. Methodology

To investigate the research question, the thesis took several approaches. First, the cybersecurity policies of the European Union and the United States were explored. To begin with, the definitions of cybersecurity and historic timelines as to when and how cybersecurity policy was addressed were compared between the EU and the U.S. After, the most current EU and U.S. legislation and policies of the United States and the European Union were analysed. On the U.S. side, legislation, and policy, such as the National Cyber Strategy of the United States, the Department of Defense Cyber Strategy, and Biden's 'Executive Order on Improving the Nation's Cybersecurity' were examined. On the EU side, the NIS Directive, the NIS2 Directive Proposal, the New EU Cybersecurity Strategy and further relevant legislation were examined. By doing this, the thesis aimed to find similarities and differences in the current EU and U.S. policies, in particular as to how assertive these policies are in the international scope. To receive further information and input regarding the legal analysis, three interviews were conducted. First, a virtual interview with Dr. Richard Harknett, a "Professor of Political Science and Director of the School of Public and International Affairs, Co-Director of the Ohio Cyber Range Institute, and Chair of the Center for Cyber Strategy and Policy at the University of Cincinnati,"[79] aided the investigation of U.S. strategy and policy on cybersecurity. Second, interviews were conducted with two IT and cybersecurity experts from Ernst and Young. One took place in Vienna with Ernst and Young's cybersecurity expert David Zacherl, and the other was conducted virtually with Lutz Naake, an Associate Partner at Ernst and Young in Munich. The two interviews with Ernst and Young aided the research by receiving more clarity on how EU legislation on cybersecurity has been adopted in the private and public sectors of various EU member states.

In addition to the legal comparison and interviews, two case studies served the purpose to analyse the limitations of the EU's and United States' current cybersecurity strategies and legislation, despite whether those are rather assertive or defensive in an international context. For the European Union, the case study "Ghost Writer" was considered. It dealt with how the EU has reacted to the involvement of Russia in cyberattacks targeting "several parliaments, officials, politicians, journalists and civil society" In 2021.[80] For the United States, the SolarWinds cyber-attack in 2020 was considered for the second case study. The significant cyberattack affected many U.S. agencies, some of them "the Pentagon, the Department of

[79] University of Cincinatti, "Richard J Harknett," Research Directory, accessed January 23, 2022, https://researchdirectory.uc.edu/p/harknerj.

[80] "EU accuses Russia of involvement in 'Ghostwriter' cyberattacks," DW, News, September 9, 2021, https://www.dw.com/en/eu-accuses-russia-of-involvement-in-ghostwriter-cyberattacks/a-59296733.

Homeland Security, the State Department, the Department of Energy," but also "private companies, like Microsoft, Cisco, Intel and Deloitte."[81] Like the case study for the EU, experts claim that this attack was orchestrated by Russia.[82] Both of these case studies were chosen because the cyber-attacks affected political institutions, an attack directly against the U.S. and EU as international actors. These attacks were, therefore, more relevant for a thesis in the discipline of international relations since the attacks did not solely affect the private sector, but also the public sector and the "states" themselves. Furthermore, it made sense to have two case studies with the same attributed attacker, Russia.

[81] Isabella Jibilian and Katie Canales, "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, April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[82] Isabella Jibilian and Katie Canales, "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."

6. Discussion

6. a. The United States

According to the U.S. Cybersecurity & Infrastructure Security Agency, "cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[83] As the usage of cyberspace advances every day, cybersecurity has indeed become a main priority in U.S. federal politics. Overall, the United States' role as a rather assertive international actor can simultaneously be seen in its cybersecurity policy and strategy. How cybersecurity policy, priorities, and strategy have developed in the United States in the past decades and up until today will be displayed in this chapter.

6. a. 1. Timeline of U.S. Cybersecurity Legislation and Policy

To provide a brief historical background on how federal cybersecurity strategy and policy has developed in the United States, James Andrew Lewis' timeline from the *Center for Strategic & International Studies*, the interview with Dr. Richard Harknett and additional primary and secondary sources will assist in providing this information.[84] Before giving a summary of how U.S. legislation has evolved up until today, one can say that policy and cyber strategy shifts in the United States have not been directly tied to an administration, but rather to conditions in cyberspace and the security the U.S. finds itself in.[85] At a first glance, it can be somewhat misunderstood since cyber policies do often speak for the character of the current administration, at least on a superficial level. This can, for example, be seen in the Trump administration's National Cyber Strategy of 2018: The language and tone of the policy are rather assertive toward great powers, such as China, which can also be said about the Trump administration itself. However, one can also argue that U.S. policymakers have recognized that cyberspace has become a strategic and tactical space that great powers use to push their own interests. It is no longer solely seen as a space of espionage, surveillance, and sabotage. This has been recognized regardless of the Trump administration and is an example of the United States' cyber strategy shift which is tied to the security the U.S. finds itself in at present.

One of the first major legislations regarding U.S. cybersecurity was the Computer Security Act which was signed by President Ronald Reagan in 1987. The Computer Security Act was one of

---

[83] "What is Cybersecurity?" Cybersecurity & Infrastructure Security Agency, last modified Nov 14, 2019, https://www.cisa.gov/uscert/ncas/tips/ST04-001.

[84] James Andrew Lewis, "Federal Cybersecurity Initiatives Timeline: Draft 1.b" Center for Strategic & International Studies, May 9, 2016, https://www.csis.org/blogs/strategic-technologies-blog/federal-cybersecurity-initiatives-timeline.

[85] Dr Richard Harknett, "U.S. Cybersecurity Policy, " interview by Lara Siebrecht, March 3, 2022.

the first important steps toward cybersecurity in the United States since it established real "guidelines" and "standards" for computer systems "for Federal computer systems."[86] In general, the Computer Security act made sure that several U.S. agencies and their employees received appropriate training for computer security, but also acknowledged the need for more coordination of cybersecurity matters with the National Security Agency.[87] One of these matters would, for example, be how to deal with "the security and privacy of sensitive information."[88] With the rise of computers and network systems, this was a crucial way toward securing the United States' computer networks for the first time. During the H.W. Bush administration, no significant other developments were found related to cybersecurity legislation, however, more progress in cybersecurity was made shortly after. President Bill Clinton's administration, for example, introduced the Presidential Decision Directive NSC-63 on Critical Infrastructure Protection. This legislation mainly had the purpose to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on [...] critical infrastructures" in both the public and private sectors.[89] Furthermore, the Critical Infrastructure Assurance Office and National Infrastructure Protection Center were created with this directive. Additionally, the Federal Computer Incident Response Capability Initiative was launched under the Clinton administration, which resulted in the opening of the Federal Computer Incident Response Center in 2003. Lastly, the Protection of National Security and Public Safety Act was passed in 1999, in which the selling of encryption products and licenses was regulated and discussed.[90] Going on to the period of about 2000 until 2015, the United States mainly focused on criminals and law enforcement in cyberspace. During this period, deterrence was also still used as the dominant response strategy. As for the George W. Bush administration, the events of the 9/11 attack very much influenced cyber strategy and policy in the U.S., in which terrorists and criminals were seen as the main enemy. A National Security Presidential Directive "to develop guidelines for offensive cyber-warfare" was designed in 2002.[91] This confirms that the United States already took an offensive approach toward cybersecurity and cyberspace twenty years ago. During the W. Bush administration, the Department of Homeland Security also released

---

[86] "H.R. 145 – Computer Security Act of 1987," Congress.Gov, accessed 17 March, 2022, https://www.congress.gov/bill/100th-congress/house-bill/145.
[87] "H.R. 145 – Computer Security Act of 1987," Congress.Gov, accessed 17 March, 2022, https://www.congress.gov/bill/100th-congress/house-bill/145.
[88] "H.R. 145 – Computer Security Act of 1987," Congress.Gov, accessed 17 March, 2022, https://www.congress.gov/bill/100th-congress/house-bill/145.
[89] "Presidential Decision Directive/NSC-63," Presidential Decision Directives -PDD, The White House Washington, May 22, 1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm.
[90] "Protection of National Security and Public Safety Act," House of Representatives, July 23, 1999, https://www.congress.gov/106/crpt/hrpt117/CRPT-106hrpt117-pt4.pdf.
[91] "National Security Presidential Directives (NSPD) George W. Bush Administration," Federation of American Scientists: Intelligence Resource Program, accessed 18 March 2022, https://irp.fas.org/offdocs/nspd/index.html.

US-CERT in 2003, a "United States Computer Emergency Readiness Team," that established initiatives such as a "National Cyber Alert System," a "National Cyber Response Coordination Group," and "Government Forum of Incident Response Security Teams."[92] During this year, the Homeland Security Presidential Directive 7 was also released with the purpose to establish "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[93] One can see here that the United States recognized how powerful non-state actors could be in cyberspace, and naturally, with Bush's war on terror, directives from the Department of Homeland Security were especially targeted toward the protection against terrorist attacks of any kind. In 2003, NSDP 38, the National Strategy to Secure Cyberspace was released, which was the very first official cybersecurity strategy in the United States. The main priorities in this document included a "National Cyberspace Security Response Team," a "National Security Threat and Vulnerability Reduction Program," a "National Cyberspace Security Awareness and Training Program," "Securing Governments' Cyberspace," and "National Security and International Cyberspace Security Cooperation."[94] What is interesting in the initial U.S. cybersecurity strategy is that the main priority seems to be improving the country's cyber defence and protecting its infrastructure. The strategy does not seem to have an offensive approach against potential competitors in cyberspace, which is seen in today's U.S. cybersecurity strategy. So, even though George W. Bush established "guidelines for offensive cyber-warfare," his cybersecurity strategy entailed a more reactive and defensive approach to secure cyberspace within the United States.[95] In 2008, the Bush administration additionally established another Homeland Security Presidential Directive (HSPD-23) in which U.S. Federal agencies' responsibility in cyberspace and security was further clarified.[96] In this directive, the word "deter" is mentioned, which again confirms that the United States did treat cyberspace as an anarchic and competitive space during the Bush administration.[97]

Moving toward the Obama administration, cyberspace was still treated as an anarchic space in which deterrence was the dominant response factor. Several times, the Cold War approach in

---

[92] "US-CERT. United States Computer Emergency Readiness Team," Homeland Security, accessed 18 March 2022," https://www.cisa.gov/uscert/sites/default/files/publications/infosheet_US-CERT_v2.pdf.
[93] "December 17, 2003 Homeland Security Presidential Directive/Hspd-7," The White House President George W. Bush, Dec 17, 2003, https://www.energy.gov/sites/prod/files/HSPD-7.pdf.
[94] "The National Strategy to Secure Cyberspace," The White House Washington," Feb 2003, https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf, x.
[95] "National Security Presidential Directives (NSPD) George W. Bush Administration," Federation of American Scientists: Intelligence Resource Program, accessed 18 March 2022, https://irp.fas.org/offdocs/nspd/index.html.
[96] "National Security Presidential Directive/NSPD-54, Homeland Security Presidential Directive/HSPD-23," The White House Washington, Jan 8, 2008, https://irp.fas.org/offdocs/nspd/nspd-54.pdf, 1.
[97]National Security Presidential Directive/NSPD-54, Homeland Security Presidential Directive/HSPD-23," The White House Washington, Jan 8, 2008, https://irp.fas.org/offdocs/nspd/nspd-54.pdf, 1.

which criminals and terrorists were seen as the main enemies proved not to be the most fitting for cyberspace during the Obama administration, for example in the "2014 North Korean hack of Sony."[98] In general, the Obama administration was rather "passive" when it came to cybersecurity strategy, which could be seen in the lack of "immediate response," "public attribution," and "diplomatic confrontation" on the U.S. side.[99] On the other hand, the U.S. publicly stated in 2015 that its cyber strategy and policy would be constrained and that the U.S. would be more careful about using cyber, which is very controversial to the Stuxnet attack. Even though the U.S. never publicly admitted its association with Stuxnet, from a U.S. point of view, the cyberattack could have been launched to leverage negotiations with the Iranians.[100] This shows that the Bush and Obama administration did slowly start to use cyberspace as a strategic and tactical space in terms of Stuxnet, even though the main strategy was based on deterrence, law enforcement and criminals in cyberspace. During Obama's first term as president of the United States, several national cyber security units were established. In 2009, for example, the National Cybersecurity and Communications Integration Center was opened, a "warning center," that is supposed to "improve national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure."[101] Additionally, the U.S. Cyber Command was established in 2009, an agency that is still very relevant today.[102] Under the first term of the Obama administration, the Department of Defense Strategy for Operating in Cyberspace in 2011 and the National Incident Response Plan in 2010 were additionally released. Especially in the Department of Defense Strategy, the U.S. made progress in recognizing the importance of partnering "with other U.S. government departments and agencies and the private sector," and building "robust relationships with U.S. allies and international partners to strengthen collective cybersecurity."[103] Especially partnering with the private sector has become an important step for securing cyberspace today. The planned collaboration with the private sector and international partners can also be seen in the scope of

[98] Foreign affairs, 14.
[99] Foreign affairs, 14.
[100] Dr Richard Harknett, "U.S. Cybersecurity Policy," interview by Lara Siebrecht, March 3, 2022.
[101] "Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center," Department of Homeland Security, Oct 30, 2009, https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened.
[102] "Memorandum For Secretaries of the Military Departments: Establishment of a Subordinate Unified U.S. Strategic Command for Military Cyberspace Operations," The Secretary of Defense, Jun 23, 2009, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf.
[103] "Department of Defense Strategy for Operating in Cyberspace," Department of Defense, July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, v.

the National Incident Response Plan.[104] Going from the first to the second term of the Obama administration, the top-secret Presidential Policy Directive 20 was signed, under which cyber operations were still treated like nuclear operations where authorization had to come directly from the president. This is also a reason why the United States under the Obama administration were not equipped to give an immediate response to cyber-attacks. This has changed today since the authorization of the president takes too long to have an effective response to a cyber incident. In 2013, the Executive Order on Improving Critical Infrastructure Cybersecurity was released, and in 2014, the National Institute of Standards and Technology "released a Framework Improving Critical Infrastructure Cybersecurity."[105] This shows that the Obama administration was prioritizing the resilience of businesses and critical infrastructure toward cyber-attacks, which means that the United States' cyber strategies and policies have not solely had an assertive nature, but also a defensive one. Toward the end of the Obama administration, further emphasis was put on a partnership with the private sector in the Executive Order on "Promoting Private Sector Cybersecurity Information Sharing."[106] Additionally, the Cyber Threat Intelligence Integration Center was established, a centre that is supposed to "provide integrated all-source intelligence analysis related to foreign cyber threats and cyber incidents affecting U.S. national interests," "support the U.S. government centers responsible cybersecurity and network defense," and "facilitate and support efforts by the government to counter foreign cyber threats."[107] The Department of Defense also released an updated Cyber Strategy in 2015 in response to the North Korean Sony cyber-attack. Here, one can see the United States' shift in operational space due to its continuous losing ground to different actors in cyberspace. As Harknett explained in the conducted interview, the U.S. around 2015 to 2016 started not to treat cyber as a space of war or single attacks, but instead acknowledged that operations in cyberspace are linked to achieving a larger goal, which could be seen in the updated Cyber strategy of the Department of Defense. Lastly, the Obama administration established the Commission on Enhancing National Cybersecurity in 2016, which is supposed to "make detailed recommendations to strengthen cybersecurity in both public and private

---

[104] "National Cyber Incident Response Plan. Interim Version," Department of Homeland Security, September 2010, https://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf, 1.
[105] "NIST Releases Cybersecurity Framework Version 1.0," NIST, Feb 12, 2014, https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10.
[106] "Executive Order – Promoting Private Sector Cybersecurity Information Sharing," the White House President Barack Obama, Office of the Press Secretary, Feb 13, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
[107] "FACT SHEET: Cyber Threat Intelligence Integration Center," the White House President Barack Obama, Office of the Press Secretary, Feb 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

sectors."[108] Overall, the Obama administration adopted many new cyber policies and initiatives, even though the administration's strategy for the most part was still fixated on an outdated approach that reminds us of nuclear deterrence. However, by the end of the Obama administration also came the critical shift from the US being a response force to the U.S. becoming a persistent force.

[108] "Executive Order – Commission on Enhancing National Cybersecurity," the White House President Barack Obama, Office of the Press Secretary, Feb 09, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

6. a. 2. The United States' Cybersecurity Strategy and Policy Today

As already mentioned, after 2015, the United States shifted away from the notion of solely seeing criminals and terrorists as the enemy in cyberspace and additionally acknowledged other actors, like great powers. Furthermore, from 2016 onward, the United States did not treat cyber as a space of war or single attacks but acknowledged that cyberspace operations are linked to achieving a larger goal. As explained in the chapter on the unique nature of cyberspace, this is known as a campaign. In this chapter, it is the thesis' aim to analyse the relevant U.S. policies and legislations that are in place today and to detect whether these have a rather proactive/assertive or reactive/defensive nature.

Since the cybersecurity legislation and policies that were formed with the Trump administration are still relevant today, the thesis will begin with cyber strategy under the Trump administration. U.S. Cybersecurity strategy and policy saw a turning point during the Trump administration since the Department of Defense and administration came to realize in 2017 that great powers use cyberspace to advance their strategic interests. This can also be seen in the White House's National Cyber Strategy of the United States of America 2018 and the Department of Defense Cyber Strategy 2018 which will be analyzed in this chapter. In these policies, it additionally becomes clear that cyberspace in the United States becomes more of a strategic and tactical space rather than a space of espionage, sabotage, and surveillance. Something that Dr. Harknett also emphasized in the interview is how the United States from 2017 onward has used "persistent engagement" in its cybersecurity strategy. Persistent engagement is the act of defending forward in cyberspace: There is a temporal element to defending forward since a persistent actor is anticipating the exploitation before it has happened. In simpler terms, to defend, one needs to be ahead of the attack. An example that Harknett mentioned in the interview related to persistent engagement and defending forward is the press. Before the acknowledgement of persistent engagement, the Department of Defense and other U.S. agencies would hide potential cyber-attacks from the press. Nowadays, however, the U.S. Cyber Command goes public, for example on the "Virus Total" website that is used to share malware information and threats. The U.S. also granted the FBI authorization to help small companies with cyber vulnerabilities in the case of a threat and works closely with the private sector to prevent exploitation before it happens. According to Harknett, persistent engagement is the way forward to deal with deterrence competitively in cyberspace. Another major legal change that happened during the Trump administration was the U.S. National Defense Authorization Act 2019 which authorized the commander of U.S. Cyber Command to move

more swiftly and rapidly when an opportunity would arise for the U.S. to exploit for its defence. As explained before, during the Obama administration, the Presidential Policy Directive 20 still treated cyber operations like nuclear operations and authorization had to come directly from the president. With the NDAA 2019, more effective and immediate responses can be made without the authorization of the president.

White House National Cyber Strategy of the United States of America 2018

Going into a deeper analysis of the policies that were formed during the Trump administration, the 'White House National Cyber Strategy of the United States of America' will be considered first. In the **introduction**, the policy takes an assertive approach, calling the United States "the world's superpower," almost romanticizing the status of the United States in the world.[109] It becomes clear here that the United States' "supremacy," its national interests and security are threatened by other actors in cyberspace.[110] As mentioned before, what is significant here is that the United States has shifted in not only recognizing non-state actors as a threat in cyberspace but also state actors. In the introduction, specific states, like North Korea, China, Russia, and Iran are called out on hiding "behind notions of sovereignty while recklessly violating the laws of other states," and harming "American and international businesses."[111] The specific mentioning of the United States' enemies in cyberspace overall takes an assertive and aggressive manner in international politics, which can perhaps also be related to the Trump administration itself. What is also rather assertive in the introduction is the way the policy promises to "aggressively address these threats and adjust to new realities," while advancing the United States' "interests across cyberspace."[112] The reason this is considered assertive/proactive is because the language of the policy is forceful and proactive toward the interests of solely the United States, not any other actors in cyberspace. The introduction also announces that the policy will "outline how" the United States will "(1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability – in concert with allies and partners – to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable,

[109] "National Cyber Strategy of the United States of America," the Trump White House Archives, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 1.
[110] "National Cyber Strategy of the United States of America," the Trump White House Archives, 1.
[111] "National Cyber Strategy of the United States of America," the Trump White House Archives 1-2.
[112] "National Cyber Strategy of the United States of America," the Trump White House Archives, 2.

reliable, and secure internet."[113] What is noticeable in this paragraph, but also the other paragraphs in the introduction is the emphasis of the word "deterrence" or "deter."[114] Even though cyber policy and strategy in the United States has shifted toward persistent engagement, it still sees deterrence as an appropriate measure to defend cyberspace. The policy claims that the United States will deter "through the imposition of costs through cyber and non-cyber means."[115] The notion of deterrence first confirms the thesis' assumption that states find themselves in an anarchic world order in cyberspace. Secondly, the United States' assertive and rather aggressive approach against its enemies in cyberspace confirms the thesis' relation of the United States toward offensive realism.

Moving toward **Pillar I** of the National Cyber Strategy, to "Protect the American People, the Homeland, and the American Way of Life," the pillar mentions three priorities, which are to "Secure Federal Networks and Information," to "Secure Critical Infrastructure," and to "Combat Cybercrime and Incident Reporting."[116] The most important aspects that are taken out of the priority to "Secure Federal Networks and Information," are the following: The administration intends to "take direct action," in overseeing "federal civilian cybersecurity," and to enable federal institutions, like the Department of Homeland Security to be more involved in cybersecurity measures.[117] Furthermore, more updated and better "federal requirements," and "information sharing" in the federal government are promised in this section.[118] This includes further cooperation with the and strengthening of federal contractors, and a standardization in "best and innovative practices" in cybersecurity.[119] As for the priority to "Secure Critical Infrastructure," the policy puts a lot of emphasis on the collaboration of the government and private sector, as well as the collaboration with information and communications technology providers.[120] Additionally, the government plans to work closely with the public and private sector in "understanding cybersecurity risks."[121] "Key areas" of "risk-reduction activities" are spread across "national security, energy and power, banking and finance, health and safety, communications, information technology, and transformation."[122] This section also prioritizes the collaboration of federal and local governments, and further

[113] "National Cyber Strategy of the United States of America," the Trump White House Archives, 3.
[114] "National Cyber Strategy of the United States of America," the Trump White House Archives, 1-3.
[115] "National Cyber Strategy of the United States of America," the Trump White House Archives, 3.
[116] "National Cyber Strategy of the United States of America," the Trump White House Archives, 6-11.
[117] "National Cyber Strategy of the United States of America," the Trump White House Archives, 6.
[118] "National Cyber Strategy of the United States of America," the Trump White House Archives, 7.
[119] "National Cyber Strategy of the United States of America," the Trump White House Archives, 7-8.
[120] "National Cyber Strategy of the United States of America," the Trump White House Archives, 8-9.
[121] "National Cyber Strategy of the United States of America," the Trump White House Archives, 9.
[122] "National Cyber Strategy of the United States of America," the Trump White House Archives, 8-9.

innovation and research in cybersecurity matters.[123] Lastly, this section points out necessary cybersecurity measures in maritime and space since these are becoming more vulnerable and exploitative in cyberspace, which could lead to economic and other consequences. The priority to "Combat Cybercrime and Improve Incident Reporting," on the other hand, emphasizes the "deterrence" of "state and non-state actors" again.[124] This time, however, cooperation with other nations, specifically, the G7 and European Union member states is suggested to prevent cybercrime and improve international law enforcement.[125] Furthermore, the section mentions the importance of incident reporting to the U.S. government. Overall, Pillar I displays the fundamental actions and collaborations that need to take place between the "federal government," "local governments," the "private" and "public sector," and "international allies." It does not necessarily have as much of an aggressive and assertive language as the introduction but is more of an instruction of how cybersecurity measures must be improved from a federal point of view.

Pillar II to "Promote American Prosperity" has the three priorities to "Foster and Protect United States Ingenuity," to "Develop a Superior Cybersecurity Workforce," and to "develop a Superior Cybersecurity Workforce."[126] Like Pillar I, Pillar II takes a rather domestic approach, but this time focuses on what can be improved in the U.S. from a technological point of view. The priority to "Foster a Vibrant and Resilient Digital Economy," pushes for more innovation development of American technologies with the purpose again to "deter and prevent current and evolving threats."[127] What is noticeable in this priority is how the U.S. builds on its "leadership" in technology and infrastructure but also focuses on "persistent engagement," to "improve resiliency ahead of the attack," which reflects the U.S. proactive/assertive character.[128] What also sheds light on its assertiveness is the policy's proactive stance for "the free flow of data and digital trade" and being ahead of competitors in matters of 5G and other technological solutions.[129] As for the priority to "Foster and Protect United States Ingenuity," this is the same case.[130] The policy specifically mentions the necessity of "maintaining the United States' strategic advantage in cyberspace," which in this priority includes the safeguarding of IP rights, potential leaks and telecommunications.[131] The last priority of this

[123] "National Cyber Strategy of the United States of America," the Trump White House Archives, 9.
[124] "National Cyber Strategy of the United States of America," the Trump White House Archives, 10-11.
[125] "National Cyber Strategy of the United States of America," the Trump White House Archives, 11.
[126] "National Cyber Strategy of the United States of America," the Trump White House Archives, 14-17.
[127] "National Cyber Strategy of the United States of America," the Trump White House Archives 14-15.
[128] "National Cyber Strategy of the United States of America," the Trump White House Archives 15-16.
[129] "National Cyber Strategy of the United States of America," the Trump White House Archives, 15.
[130] "National Cyber Strategy of the United States of America," the Trump White House Archives 16.
[131] "National Cyber Strategy of the United States of America," the Trump White House Archives 16.

pillar, to "Develop a Superior Cybersecurity Workforce," also promotes the improvement of technology in the United States by investing in workforce "talent."[132] This does not only mean fair and better recruitment, but also "re-skilling people from a broad range of backgrounds," which, like the other priorities of this pillar, showcases the United States' efforts to have a strategic advantage over its competitors and its assertive character.[133]

Pillar III, and IV to "Preserve Peace through Strength," and to "Advance American Influence," display the United States' priorities from an international point of view.[134] Already at the beginning of Pillar III, one can observe that the United States sees cyberspace as a space of "strategic balance of power," in which "deterrence" is the appropriate measure, and confirms the theoretical framework of realism.[135] Deterrence is often mentioned in the second priority of Pillar III, to "Attribute and Deter Unacceptable Behavior in Cyberspace," where the United States takes a very assertive and leading stance against "malicious cyber activity," but also promotes collaboration with its allies to deter and "impose consequences" to malicious actors in cyberspace.[136] The United States' efforts to collaborate with allies in cyberspace can also be seen in Pillar IV in the priority to "Build International Cyber Capability."[137] Here, it becomes clear, however, that the US intends to maintain "American influence," and lead the "Cyber Deterrence Initiative" while doing this.[138] The policy furthermore promotes universal norms in cyberspace in the priority to "Enhance Cyber Stability through Norms if Responsible State Behavior," and the partnership of "like-minded countries, academia, and civil society," as well as international organizations in governing and operating the internet and cyberspace.[139] In Pillar III and IV, the United States takes proactive leadership in introducing norms, partnering with allies, and deterring malicious cyber activity in the international realm, which strongly underlines its assertive character in cyberspace.

Overall, the White House National Cybersecurity Strategy 2018 confirms what was expected in this thesis: The United States is not only an assertive and proactive international actor in general but also takes this approach in cybersecurity policy. This can be seen in the country's persistent engagement strategy and strategic efforts to be technologically ahead of its competitors in cyberspace. Additionally, the United States takes international leadership in securing cyberspace for primarily American interests.

---

[132] "National Cyber Strategy of the United States of America," the Trump White House Archives, 17.
[133] "National Cyber Strategy of the United States of America," the Trump White House Archives 17.
[134] "National Cyber Strategy of the United States of America," the Trump White House Archives, 20-26.
[135] "National Cyber Strategy of the United States of America," the Trump White House Archives 20.
[136] "National Cyber Strategy of the United States of America," the Trump White House Archives, 21.
[137] "National Cyber Strategy of the United States of America," the Trump White House Archives, 26.
[138] "National Cyber Strategy of the United States of America," the Trump White House Archives, 26.
[139] "National Cyber Strategy of the United States of America," the Trump White House Archives, 20.

Department of Defense Cyber Strategy 2018

The Department of Defense Cyber Strategy 2018 is, naturally, similar to the White House National Cybersecurity Strategy 2018. The introduction, for example, has many of the same elements. First, the notion of deterrence is mentioned. The Department of Defense states here that it "seeks to preempt, defeat, or deter malicious cyber activity," but also, like the National Cyber Strategy, mentions persistent engagement and the importance of "defending forward."[140] Second, the DoD Strategy actively calls out competitive state actors whom the United States sees as a threat. These would again be Russia, China, Iran, and North Korea. Third, the strategy sees cyberspace as a competitive space in which the U.S. and other actors seek to advance their own interests. And fourth, the strategy promotes collaboration and work with "U.S. allies and partners to strengthen cyber capacity."[141] The difference between the DoD and the National Cyber Strategy is the military aspect. The Department of Defense sees cyberspace, for example, as a domain in which wars can potentially be fought and therefore intends to "ensure the U.S. military's ability to fight and win wars in any domain, including cyberspace."[142] This is also confirmed in the DoD Strategy's conclusion, in which it mentions that the Department of Defense will "defend forward, shape the day-to-day competition, and prepare for war."[143]

Compared to the National Cyber Strategy, the DoD Strategy is more precise in how the U.S. will militarily compete and dominate in cyberspace. After the Department of Defense mentions its main objectives in cyberspace, it moves on toward the strategic approach in how those objectives will be fulfilled.[144] The main points in the strategic approach are to "build a more lethal joint force," to "compete and deter in cyberspace," to "strengthen alliances and attract new partnerships," to "reform the department," and to "cultivate talent."[145] What sets the DoD Strategy apart from the National Cyber Strategy is the goal to "build a more lethal joint force" and to "reform the department."[146] These two points are more applicable for Department of Defense itself. However, the two strategic approaches also have the same goal as any of the other approaches: "to advance U.S. interests."[147] To achieve this, the Department of Defense,

[140] "Summary Department of Defense Cyber Strategy," Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, 1-2.
[141] "Summary Department of Defense Cyber Strategy," Department of Defense, 2.
[142] "Summary Department of Defense Cyber Strategy," Department of Defense, 2.
[143] "Summary Department of Defense Cyber Strategy," Department of Defense, 7.
[144] "Summary Department of Defense Cyber Strategy," Department of Defense, 3-4.
[145] "Summary Department of Defense Cyber Strategy," Department of Defense, 4-6.
[146] "Summary Department of Defense Cyber Strategy," Department of Defense, 4-5.
[147] "Summary Department of Defense Cyber Strategy," Department of Defense, 4.

like the National Cyber Strategy, relies on persistent engagement, innovation, deterrence, resilience, and internal cyber awareness.[148]

Something that is worth mentioning is how the DoD Strategy states in its conclusion how the United States will "assertively defend" cyberspace. This can be connected to the remarks of Dr. Harknett in the conducted interview: He stated that to defend to the fullest capacity in cyberspace, one must at the same time have an offensive/assertive approach. This has clearly also been adopted in U.S. military strategy in cyberspace, and in terms of U.S. cyber strategy, offense and defence go hand in hand.

President Biden's Executive Order on Improving the Nation's Cybersecurity and the Future of U.S. Cyber Policy and Strategy

Lastly, as for current U.S. policy and strategy, the thesis will take President Biden's Executive Order on Improving the Nation's Cybersecurity into consideration and will briefly discuss where U.S. cybersecurity strategy is heading in future. Overall, it is noticeable how this policy order is not as assertive as the National Cyber Strategy 2018. For example, the policy order does not use the word "deterrence" as much and does not call out specific enemies in cyberspace. The policy rather suggests appropriate measures which can be executed on a domestic level for U.S. agencies and government to obtain improved cyber defence capabilities.

Section 1 on "Policy" in Biden's Executive Order on Improving the Nation's Cybersecurity provides the "scope of protection and security" which includes information technology and operational technology. **Section 2** on "Removing Barriers to Sharing Threat Information" overall displays the importance of the partnership between the Federal Government and private sector, but also aims to share more information and to remove barriers between various U.S. agencies and the government for more effective "incident deterrence, prevention, and response efforts" (Sec. 2, a). This section furthermore ensures that service providers share more data, information and threats with U.S. agencies and the Federal Government (Sec. 2, c, i-iv). It also ensures that "ICT service providers report cyber incidents to agencies" (Sec. 2, f), the sharing of cyber incident reports among agencies (Sec. 2, g), and standardization of cybersecurity requirements among agencies (Sec. 2, h) that will be updated regularly (Sec. 2, j). **Section 3** on "Modernizing Federal Government Cybersecurity" focuses on modernizing cybersecurity through cloud services, such as SaaS, IaaS, PaaS, and Zero Trust Architecture (Sec. 3, a-b). Cloud technology is supposed to be adopted on a federal and U.S. agency level, which will

[148] "Summary Department of Defense Cyber Strategy," Department of Defense, 4-6.

include training programmes and incident response activities (Sec. 3, c-f). **Section 4** on "Enhancing Software Supply Chain Security" ensures more security for "critical software," improvements of the integrity and security of "the software supply chain," and puts emphasis on working together with the private sector and academia while doing this (Sec. 4, a-c). Furthermore, this section prioritizes that "critical software" will be defined and categorized, so that U.S. agencies will be able to comply with specific requirements and standards of using and testing software (Sec 4, g-r). On top of this, "secure software development practices" and programmes will be implemented for reviewing purposes (Sec 4, u-w). **Section 5** on "Establishing a Cyber Safety Review Board" already says the purpose of this section in itself: It will create a cybersecurity review board that will consist of federal and private sector representatives, as well as U.S. agencies (Section 5, c-f). The board will give "recommendations to the Secretary of Homeland Security" who will report to the president on cybersecurity-related matters (Sec. 4, d-h). Moving on to **Section 6**, "Standardizing the Federal Government's Playbook for Responding to Cybersecurity," this section ensures a more standardized response to cyber incidents and will "develop a standard set of operational procedures (playbook) to be used in planning and conducting a cybersecurity vulnerability and incident response activity" (Sec. 4, a-b). This "playbook" will be used mostly for U.S. agencies and will be updated regularly (Sec. 4, b-f). **Section 7** on "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks" has the intention to "maximize the early detection of cybersecurity vulnerabilities," and therefore to implement an "Endpoint Detection and Response (EDR) Initiative" which will "support proactive detection of cybersecurity incidents" (Sec 7, a-d). This section also mentions "appropriate actions" for detecting cyber incidents, such as "threat-hunting activities," and implementing a "notifying system" (Sec 4, e-g). **Section 8** on "Improving the Federal Government's Investigative and Remediation Capabilities" mainly ensures the provision of "recommendations and requirements for logging events" and "recommended logging ad security requirements," while retaining data, which will be given to the Secretary of Homeland Security (Sec. 8, b-e). Lastly, **Section 9** on "National Security Systems" already says in itself that National Security Systems must be adopted (Sec. 9, a). The last part of the Executive Order provides definitions and general provisions (Sec. 10, 11).

As already mentioned, the 'Executive Order on Improving the Nation's cybersecurity' suggests appropriate measures that can be executed on a domestic level for U.S. agencies and government to obtain improved cyber defence capabilities. So, perhaps one can draw from this that cybersecurity measures in general always have a defensive tone, even for a rather assertive international actor, like the United States. As Dr Harknett mentioned, cybersecurity policy, like

any other matter in U.S. politics, will always slightly change, but not to a large extent. Cybersecurity policy rather changes due to the circumstances the country finds itself in.

Speaking of cybersecurity, current President Biden seems to understand the changes that need to be addressed, which are, as one can see in his Executive order, many technical ones from a federal point of view. Internal cyber resilience is as important as taking an assertive/proactive international stance in cyberspace. The thesis, however, suggests that this recognition of needed change would have come eventually, no matter which administration would have been in office. Also, during the Trump administration, many significant, strategic changes were made in cybersecurity policy and strategy, which shows that changes in cybersecurity policy do not completely depend on the president, but mostly on the development of cyberspace and the cybersecurity that is required. For example, just recently, the U.S. Senate just recently passed new legislation on cybersecurity, the Strengthening American Cybersecurity Act of 2022, "requiring 72 hour cyber incident notification."[149] Before this bill, no federal bills really existed on cybersecurity as mostly states ran their own cybersecurity regulations. This is a sign that the U.S. federal government is taking more leadership in cybersecurity issues, as the threats of cyberspace have made the U.S. more vulnerable, which does not completely relate to the administration that is currently in place. As for where cybersecurity policy is further headed in the United States, one can see that the Federal Government has made many adjustments in the past decades. For example, the U.S. has shifted from solely seeing criminals and terrorists as the enemy in cyberspace and has additionally acknowledged other states as a threat. Furthermore, the United States now recognizes that there is a larger strategic goal in various cyber-attacks, which are known as campaigns. The United States has recognized cyberspace as a strategic space in which states and non-state actors use to advance their own interests. To operate in this space, the U.S. now additionally uses persistent engagement on top of deterrence, which also proves that the U.S. has come to understand that cyberspace is an exceptional military space and cannot be compared to conventional military spaces. Especially considering the Russian invasion in Ukraine, CISA, U.S. agencies, companies and the U.S. government are on the highest alert for any potential cyber-attacks coming from Russia. This will only speed up the progress that has developed in the past twenty or so years in U.S. cybersecurity policy.

[149] "U.S. Senate Unanimously Passes Cybersecurity Legislation Requiring 72 Hour Cyber Incident Notification," The National Law Review, Volume XII, Number 100, April 10, 2022, https://www.natlawreview.com/article/us-senate-unanimously-passes-cybersecurity-legislation-requiring-72-hour-cyber.

6. a. 3. Case Study: SolarWinds Cyber-Attack

To finish the analysis on U.S. cybersecurity policy, the thesis will provide a short case study on the SolarWinds cyber-attack in 2020 and relate the attack to current U.S. cybersecurity strategy and efforts. SolarWinds is a company based in Texas that produces software for its clients "to help manage their networks, systems, and information technology infrastructure."[150] In December 2020, the cyber-security company FireEye found that it had been hacked by an unknown, but powerful actor. The company additionally found that SolarWinds was the transmitter of the cyber-attack and that many undetected hacks had taken place. The SolarWinds cyber-attack was a "supply chain attack," that was linked to the "SolarWinds Orion Platform," a management platform that was used by many of the company's clients.[151] In an update of the Orion Platform, the attackers added malicious code in an attachment, which was sent out to SolarWinds' clients. When clients downloaded the malware, the attacker was able to access many of the clients' email and Microsoft accounts. The reason this attack was so significant and had major consequences is because many large companies from the private sector, but mostly U.S. agencies were strongly hit by it. For example, the U.S. Department of Treasury, Department of Homeland Security and Department of Health were victims of the SolarWinds cyber-attack. In total, 18,000 clients downloaded the malware, of which some were high security officials.[152] Furthermore, the attack had gone unnoticed for several months since the software update was sent out in March 2020. This means that the attacker was most likely able to steal a lot of information since it was a longer unnoticed timeframe. In a financial sense, the repair costs of the attack lie at about 40 million U.S. dollars.[153]As of now, the suspect of the SolarWinds cyber-attack is still either Russia or China, although the current administration leans more toward Russia.

The question is how the SolarWinds cyber-attack relates to the discussion on U.S. cybersecurity policy and strategy. After the cyber-attack had been detected, the current Biden administration

---

[150] "Moving IT forward," SolarWinds, accessed April 5, https://www.solarwinds.com/homepage-3c?adobe_mc_sdid=SDID%3D3E840169ABD6542B-633360A32EB97B8B%7CMCORGID%3D8D6867C25245AEFB0A490D4C%40AdobeOrg%7CTS%3D1649333489&adobe_mc_ref=https%3A%2F%2Fwww.google.com.

[151] "One vendor. One platform. One single pane of glass." SolarWinds, Orion Products, accessed 5 April 2022, https://www.solarwinds.com/solutions/orion.

[152] Marcus Willett, "Lessons of the SolarWinds Hack," *Global Politics and Strategy,* vol. 63, issue 2, 30 March 2021, https://www.tandfonline.com/doi/full/10.1080/00396338.2021.1906001.

[153] Samantha Schwartz, "One year later: has SolarWinds changed how industry builds software?" Cybersecurity Dive, Dec 14, 2021, https://www.cybersecuritydive.com/news/solarwinds-1-year-later-cyber-attack-orion/610990/.

announced to launch a serious, "several months" long investigation into the attack.[154] Furthermore, the Biden administration attributed the attack to Russia after further investigation and formalized sanctions against the country. Lastly, President Biden has tried to improve cybersecurity measures within the U.S., which can be seen in his 'Executive Order on Improving the Nation's Cybersecurity.' With this said, one can see that the SolarWinds attack was an unexpected cybersecurity breach that proved that the United States' cybersecurity measures were not effective enough. Even though the previous Trump administration formed an assertive cybersecurity strategy that distinctly threatened to deter states, like China, Russia, Iran, and North Korea, the SolarWinds attack was very successful. The SolarWinds attack might be the perfect example that deterrence and an assertive cybersecurity strategy might not be enough to secure cyberspace. For example, the United States' threats of deterrence could not prevent the attack. Second, one can only effectively deter when there is an attributed attacker. For some time, the United States was unsure whether the actor behind the SolarWinds attack was Russia or China, which took too much time to deter effectively. As for persistent engagement, the strategy is probably the most effective when as many entities from not only the government and government agencies but also the private and public sectors are aware of it. In the case of the SolarWinds attack, one could see that the government and private sector were not very well coordinated with one another, which leads to many vulnerabilities in cyberspace. From Biden's 'New Executive Order on Improving the Nation's Cybersecurity,' one can draw that the communication and information sharing between the government, its agencies and the private sector were lacking, which will be improved in future. So, perhaps the following remarks can be drawn from the SolarWinds case study: It seems that in order to secure a state's cyberspace, measures need to be taken to improve the state's internal strength and resilience against cyber-attacks. An example of this is a strong partnership between the government, the private and public sectors. Another example of this is eliminating vulnerabilities in all potential victims of cyber-attacks, which means promoting more awareness and education on cybersecurity within all relevant sectors and government agencies. Furthermore, another point that can be drawn from this case study is that an assertive/proactive cybersecurity strategy might be effective, however, it highly depends on what way the state-actor is proactive. Perhaps assertiveness and proactiveness need to be not only tied to deterrence and persistent engagement within the government but must be linked to proactive communication and strategy sharing with the private sector and U.S. allies. Lastly, as already

[154] Brian Fung, "Biden administration says investigation into SolarWinds hack is likely to take 'several months,'" CNN Politics, Feb 17, 2021, https://edition.cnn.com/2021/02/17/politics/solarwinds-hack-investigation/index.html.

mentioned, deterrence is effective, but only if the actor responsible for the attack can be attributed.

6. b. The European Union

According to the European Union Agency for Cybersecurity, "Cybersecurity shall refer to the security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. "[155] Also, within the European Union, cybersecurity seems to become more of a priority as technology advances in our world. Like with the United States, this chapter will provide an analysis of how cybersecurity policy, priorities, and strategy has developed within the European Union over the past decades up until today

6. b. 1. Timeline of EU Cybersecurity Legislation and Policy

Like with the United States, a brief background will be provided on how cybersecurity policy and legislation have developed in the European Union. Before touching on EU legislation and policy that has been developed so far, it is important to point out that many policies and legislations exist in the EU that are "multi-layered," and overlapping, which can often lead to confusion while compiling all documents that are related to cybersecurity.[156] For this reason, the thesis will mention legislation and policies that it considers relevant, however, will not include every single document that has somewhat related to IT in the EU. Furthermore, the first cybersecurity initiatives within the European Union did not take place as early as in the United States, which is why the timeline of EU cybersecurity legislation and policy is narrower than on the U.S. side. Overall, the European Union's approach toward cybersecurity developed differently and later than the one of the U.S. From the beginning, the European Union's legislation on cybersecurity had more weight in the actual defence and resilience of European cyberspace. Cyber strategy, policy and legislation was not assertive in the international community. However, this might also be due to the general fact that the European Union has never had a hegemonic international stance, like the United States and other great powers, such as Russian and China. However, like the United States, the European Union similarly recognised non-state actors, such as terrorists as the main threat in cyberspace. This has gradually changed, though. In more current policy and statements, the EU makes it clear that

---

[155] "Definition of Cybersecurity – Gaps and overlaps in standardisation," ENISA European Union Agency for Cybersecurity, Publications, July 1, 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity, 7.

[156] "Challenges to effective EU cybersecurity policy: Briefing Paper," European Court of Auditors, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf, 12.

great powers, like Russia and China, have become significant threats in cyberspace. As in the case of the United States, it also seems to be that policy and cyber strategy shifts within the European Union have not been directly tied to an administration or leadership positions, but rather to conditions in cyberspace and the security the EU finds itself in.

The first legislation that was ever passed regarding cybersecurity in European states was the Budapest Convention on Cybercrime in 2001, which was led by the Council of Europe. Its main objective was "to pursue a common criminal policy aimed at the protection of society against cybercrime."[157] In 2002 until 2005, other legislations were developed, such as the "Common Framework for Electronic Communications Networks and Services," the legislation on "Combatting fraud and counterfeiting of non-cash means of payments," and the "Council Framework Decision on attacks against information systems"[158] Furthermore, ENISA, the European Union Agency for Cybersecurity was created in 2004, a fundamental agency for cybersecurity in the EU that would later become an important part of the Network and Information Security Directive (NIS Directive) and Cybersecurity Act that are still in place today.[159] As one can observe, however, the legislations up until 2005 were a rather broad framework and orientation as to how member states should deal with cybersecurity on a national level. Shortly after, in 2007, the EU had its first big awakening about the impact cyber-attacks could have on an EU member state. Only three years after Estonia joined the European Union, it was hit by a large amount of "cyber-attacks, information warfare," and "fake news," in which the Russian government is still assumed to be the attributed attacker since Estonia at the time was removing a Soviet memorial.[160] Immediately, in 2008, the Estonian government implemented a National Cyber Security Strategy and has since then has had the strongest cybersecurity strategy implementation of all member states in the EU.[161] What is noticeable here is that the main reaction to what had happened in Estonia mainly came from NATO, and not the EU, which hints toward the fact that the EU was at this stage lagging behind great powers, such as the US, in terms of implementing an effective and relevant cyber-security strategy. Only in 2011, EU member states began to implement a national cybersecurity strategy,

---

[157] "Details of Treaty No. 185," Council of Europe Portal," Treaty Office, accessed 29 March 2022, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.
[158] "Challenges to effective EU cybersecurity policy: Briefing Paper," European Court of Auditors, 11.
[159] "NIS-Directive," ENISA European Union Agency for Cybersecurity, Topics, accessed 28 March, 2022, https://www.enisa.europa.eu/topics/nis-directive.
[160] Damien McGuiness, "How a cyber attack transformed Estonia," BBC News, 27 April 2017, https://www.bbc.com/news/39655415.
[161] "2007 cyber attacks on Estonia," Stratcomcoe, 2007, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf, 55.

for example, Germany, Great Britain, France, the Netherlands, Lithuania, the Czech Republic, and Luxembourg. Other member states followed in the years after. However, slowly the European Union recognized the importance of protection in cyberspace and implemented further legislation, such as the "Identification and designation of European critical infrastructures and the assessment of the need to improve their protection" in 2008, an "Update of ENISA Regulation" in 2011 and the "Establishment of CERT-EU" in 2011, the Computer Emergency Response Team in the EU.[162] ENISA has in this timeframe and up until today become an important agency that is responsible in aiding EU member states, but also EU institutions and agencies in implementing cyber and IT security standards. Next to ENISA, CERT EU is a "permanent response team" responsible "for the EU institutions, agencies and bodies," and "is made up of IT security experts from the main EU Institutions."[163]

The "cornerstone" of EU cybersecurity policy, however, was the "2013 Cybersecurity Strategy," in which the main priorities were "cyber resilience," "reducing cybercrime," "developing defence policies and capabilities," "developing industrial and technological cybersecurity resources," and "establishing an international cyberspace policy aligned with core EU values."[164] The strategy is supposed to go hand-in-hand with further digital EU policies, such as the "European Agenda on Security," 2015 the "Digital Single Market Strategy" 2015, and the "2016 Global Strategy."[165] In 2013, the European Cybercrime Centre was additionally established, short, known as EC3. The EC3 rather focuses on "cyber-dependent crime," unlike the other agencies that focus on cybersecurity standards within the EU.[166] The EC3 was founded by Europol "to help protect European citizens, businesses and governments from online crime."[167]In 2014, the first "Cyber Defence Policy Framework" was adopted and had the main objective to find "priority areas" in cybersecurity for the Common Security and Defence Policy of the EU.[168] The EU Cyber Defence Policy Framework was a "response to the need to step up EU cyber resilience," and launched "a dedicated training and education platform […] to support cyber defence training opportunities offered by Member States" and promoted the development

---

[162] "Challenges to effective EU cybersecurity policy: Briefing Paper," European Court of Auditors, 11.
[163] "About us," CERT-EU, accessed 01 April, 2022, https://cert.europa.eu/cert/plainedition/en/cert_about.html.
[164] "Challenges to effective EU cybersecurity policy: Briefing Paper," European Court of Auditors, 12.
[165] "Challenges to effective EU cybersecurity policy: Briefing Paper," European Court of Auditors, 12.
[166] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[167] "European Cybercrime Centre – EC3: Combating crime in a digital era," Europol, last updated 01 March 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
[168] "Outcome of Proceedings: EU Cyber Defence Policy Framework," 18 Nov 2014, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf, 2.

of projects related to cyber defence.[169]An updated version of this document was released in 2018 and will be discussed further in the next section of this chapter. In addition to this, the EU has established a "Joint Framework on countering hybrid threats" in 2016, in which the EU "tackles cyber threats to both critical infrastructure and private users."[170] Here, the EU has also tried to cooperate as much as it can with NATO. As already mentioned, something that is noticeable on the EU side of cybersecurity policy and legislation is that up until today, NATO has mainly taken initiative in terms of cybersecurity strategy and implementation. The EU itself, however, has started to increase initiatives, legislation, and policy in terms of cybersecurity and data protection in the past years. These will be considered in more detail in the next section of this thesis.

[169] "Cyber defence: Council updates policy framework," European Council, Council of the European Union, 19 Nov 2018,https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/.
[170] "Challenges to effective EU cybersecurity policy: Briefing Paper," European Court of Auditors, 13.

6. b. 2. The European Union's Cybersecurity Strategy and Policy Today

In past years, the European Union has progressed in forming various legislation and policies regarding cyberspace and data regulation. It is noticeable how the EU is shifting its priorities toward matters of technology. Still, unlike the United States, the European Union has not explicitly recognized cyberspace as a strategic space that it can use to gain advantages over others. In the following legislation that will be analysed, the EU rather acknowledges areas that need to be protected and is not very proactive in dominating cyberspace from a strategic point of view. Therefore, the thesis sees the European Union can be as a rather defensive/reactive actor in cyberspace.

NIS Directive

The Network and Information Security Directive (NIS Directive) is considered the first official cybersecurity and IT security directive in the European Union and was released in 2016. It is the EU's framework for information security. Because the NIS Directive is a directive, each EU member state could decide how to adopt it in its own national legislation, which gave member states a lot of freedom. According to ENISA, the agency that plays a role in "aiding member states to implement the NIS Directive," "the national transposition by the EU member states happened on 9 May 2018."[171]

Before analysing the actual directive, a few observations will be mentioned about the preamble of the NIS Directive. In the preamble, the European Union realizes that there is a need for a strategy and "minimum capabilities" in cyberspace among member states and acknowledges these gaps (§4-5). Furthermore, the preamble states that "operators of essential services and digital service providers" will be affected by the directive (§7), but this is also very broad since it is up to the member state which companies are categorized as such (§19-20, 25). The interviews with Mr Naake and Mr Zacherl confirmed that the NIS Directive is rather vague in terms of which companies and institutions are affected by the directive. In addition, the preamble gives provisions of what each member state must implement in terms of cybersecurity and the role ENISA plays in this (§29-38). This information, however, is more specific in the actual directive. The preamble also sees "operators of essential services" at a higher risk than "digital service providers" (§49). In terms of deterrence, nothing is mentioned. In fact, the preamble has a rather reactive/defensive tone from an international relations perspective which can be seen in §34, "to prevent, detect, respond to and mitigate network and information system incidents and risks," and §46 "to prevent, detect and handle incidents." Here, nothing proactive

[171] "NIS-Directive," ENISA European Union Agency for Cybersecurity.

is mentioned regarding the European Union gaining a strategic advantage over other actors in cyberspace. However, the preamble does promote "international cooperation to improve security standards," (§43) but does not mention specifically with whom it will cooperate.

As for the actual NIS Directive, ENISA states that it has "has three parts," which are divided into "national capabilities," "cross-border collaboration," and "national supervision of critical sectors."[172] In terms of **national capabilities**, member states must have "a national strategy on the security of network and information systems" (Art. 7). This includes "strategic objectives and appropriate policy and regulatory measures" (Art. 7, §1), a "national single point of contact," (Art. 8), more education, training programmes and research in IT security, and a risk assessment plan (Art. 7, §1d-g). Furthermore, the directive promotes cooperation between national governments and the private and public sectors (Art.7, §1a-c). The affected companies that are "operators of essential services" and "digital service providers" have certain "security and notification requirements" (Art. 1, a-d). Furthermore, the directive requires each member state to have "computer security incident response teams (CSIRTs)" (Art. 9). These are supposed to "monitor incidents at a national level," provide "early warning, alerts, announcements and dissemination of information," respond "to incidents," and provide "dynamic risk and incident analysis and situational awareness" (Annex 1, §2).

In terms of **cross-border collaboration**, the NIS Directive establishes a "Cooperation Group" (Art. 11) and a "CSIRTs network" (Art. 12), while promoting "international cooperation" (Art.13). The Cooperation Group, on the one hand, is established for exchanging information and building trust among member states (Art. 11, §1) and is "composed of representatives of Member States, the Commission and ENISA" (Art. 11, §2). Its tasks include guiding CSIRTs, as well as "best practice" experience, and risk assessment exchanges among member states (Art. 11, §3). Furthermore, the Cooperation Group now has "a work programme in respect of actions to be undertaken to implement its objectives and tasks." (Art. 11, §4-5). The CSIRTs network on the other hand, "is composed of representatives of the Member States' CSIRTs and CERT-EU," and, likewise, promotes more trust and cooperation among member states (Art. 12, §1-2). The tasks of the CSIRTs network include information exchange on "CSIRTs services," incidents, risks, investigations while promoting further forms of "operational cooperation" (Art. 12, §3a-f). Furthermore, the CSIRTs network communicates closely with the Cooperation Group and discusses "lessons learnt from exercises relating to the security of network and information systems, including those organised by ENISA" (Art. 12, §3g-j). In terms of

[172] "NIS-Directive," ENISA European Union Agency for Cybersecurity.

international cooperation, the directive encourages international agreements with international organizations and third countries (Art. 13).

As for the **national supervision of critical sectors**, the NIS Directive addresses member states' own "identification of operators of essential services" (Art. 5), "security requirements and incident notification" for "operators of essential services" (Arts.14-15) and "security requirements and incident notification" for "digitals service providers" (Arts. 16-17). According to Article 5 and Annex 2, operators of essential services belong to sectors of "energy," "transport," "banking," "financial and market infrastructures," the "health sector," "drinking water supply and distribution," and "digital infrastructure." However, because member states can identify themselves which operators of essential services apply to the NIS Directive, the implementation of this has varied very much among member states. This is the same case for digital service providers: Annex III is likewise very vague in identifying the "types of digital services" which are an "online marketplace," an "online search engine," or a "cloud computing service." However, national supervisions for "digital service providers" apply to all digital service providers that have a "main establishment in a Member State," even if the provider has not been established within the European Union (Art. 18, §1-3). Something that is noticeable in the "security requirements and incident notification" is how the notification takes place after a cyber incident has occurred. This, of course, is logical, however, no notion can be identified in the NIS Directive regarding persistent engagement, e.g., anticipating the attack before it has even happened. This again confirms the rather reactive/defensive nature of the NIS Directive.

After interviewing Bernard Zacherl and Lutz Naake from Ernst and Young Vienna and Munich, more can be said about how the NIS Directive has played out in practice. What has been observed by both cyber and IT experts in Austria and Germany is that the NIS Directive was generally too vague and crude, which led to very different local laws, but also very different implementation of cyber and IT security implementation among EU member states. For example, in Hungary, 250 companies were affected by the NIS Directive, whereas in Finland the number was 4000, which is a significant difference. Something else that has been observed is how rather big EU member states that contribute toward most of the EU budget, like Germany and France, have implemented the NIS Directive more strictly than other EU member states. Interviewing cyber and IT security experts from two different EU member states that vary in size and the role they play in the EU was useful since one can see how the NIS Directive has been implemented on a national level from two perspectives. From a German perspective, an IT Security law (IT-Sicherheitsgesetz) was already implemented in 2015 before the NIS

Directive was published in 2016. Furthermore, Germany has a "KRITIS" IT law (KRITIS IT-Gesetz) since 2017 that assigns thresholds, as well as sectors in IT security of critical infrastructures. Additionally, the Institute of Public Auditors in Germany (IDW), with the support of the BSI, has created a catalogue of requirements for the concretization of KRITIS Not only does Germany's advanced law set the country apart from other EU member states in IT security, but also the obligation for firms to be audited every two years. Stricter auditing does not take place in most EU member states, which leads to many European companies not having good enough IT security requirements. In fact, many EU member states, including Austria, strive to receive an ISO-27001 certification, which is from the non-profit organization "International Organization for Standardization." The ISO-27001 certification provides "best practice standards" for IT security. The problem with this certification is that no official audits need to be conducted and thus companies can easily fake IT security standards. Austria itself was not as advanced in IT and cyber security implementation as Germany. For example, the companies that are affected by the NIS Directive will triple soon with the upcoming NIS Directive II, which will be further discussed in this section of the thesis. Overall, the vague implementation conditions in the NIS Directive have led to many cyber and IT security gaps within the member states of the European Union.

Something that is important to add here is that the very different implementation of cyber security standards can also be connected to EU institutions and agencies themselves, not just member states. A recent report from the European Court of Auditors just recently announced that "EU institutions, bodies and agencies (EUIBAs) have very different levels of cybersecurity maturity and do not always comply with good practice."[173] This hints toward the fact that ENISA and CERT-EU must focus more on aiding EU institutions next to member states in implementing appropriate cyber and IT security standards and that the European Union itself still has a long way to go in terms of cybersecurity standards.[174] In conclusion of the NIS Directive, it was noticeable how this legislation was rather defensive and had a reactive tone, rather than an assertive or proactive one. The legislation prioritised cyber and IT security measures and, in fact, did not mention anything about proactively gaining an advantage over other actors in cyberspace, unlike the United States. The NIS Directive, therefore, confirms the thesis' assumption that the EU is a rather defensive/reactive international actor in cyberspace.

---

[173] "Special Report. Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats," European Court of Auditors, 2022, https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_EN.pdf, 2.

[174] "Special Report. Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats," European Court of Auditors, 5.

NIS2 Directive

While the NIS Directive was the first legislation within the European Union that made member states have a certain level of cybersecurity, it also proved to have many gaps, especially in terms of the various implementation of the directive. Therefore, the European Commission released a proposal for a renewed version of the legislation in 2020 called the NIS2 Directive. The NIS2 Directive is supposed to "strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU."[175] Furthermore, the new version of the directive will oblige "more entities and sectors to take measures," which will "assist in increasing the level of cybersecurity in Europe in the longer term."[176] The obligation for more companies to take measures according to the NIS Directive can, for example, be seen in Austria: the number of companies that will be affected by the NIS2 Directive will triple compared to the initial NIS Directive from 2016. After an evaluation of the initial NIS Directive, the EU Commission found that the NIS Directive had several gaps: The "scope of the NIS Directive was too limited;" There was not enough "clarity" in terms of which "digital service providers and operators of essential services" were affected; "Security and incident" reporting measures varied too much among member states; "The supervision and enforcement regime of the NIS Directive" were "ineffective;" And the proposed information sharing of cyber security measures among member states did not go as planned.[177]Therefore, the NIS2 Directive has the main objective of including more "entities and sectors to take measures," while improving "national supervision and enforcement," and increasing cooperation among member states as well as the entities that are affected by the NIS2 Directive.[178] Next to this, a "review of the Resilience of Critical Entities (CER) Directive" and initiatives on "a digital operational resilience act for the financial sector," and on "a network code on cybersecurity with sector-specific rules for cross-border electricity flows" will take place.[179] As one can see, the EU has recognized major gaps in the initial NIS Directive and will especially work toward the concretization of affected companies and entities, which is beneficial for IT and cyber security in the European Union. It will also review and eventually

[175] "The NIS2 Directive: A high common level of cybersecurity in the EU," European Parliament Think Tank, Briefing, 01 Dec 2021, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.
[176] "The NIS2 Directive: A high common level of cybersecurity in the EU," European Parliament Think Tank."
[177] "The NIS2 Directive: A high common level of cybersecurity in the EU," Briefing, EU Legislation in Progress, Dec 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, 6.
[178] "The NIS2 Directive: A high common level of cybersecurity in the EU," Briefing, EU Legislation in Progress, 7-8.
[179] "The NIS2 Directive: A high common level of cybersecurity in the EU," Briefing, EU Legislation in Progress,, 8.

release new legislation in related fields, such as critical infrastructures. However, despite many of the EU's efforts, it will still be difficult to overcome cyber and IT security gaps. For example, one of the main issues that were discussed in the conducted interviews was the fact that the EU does not require member states to perform stricter audits on affected entities by the NIS Directive. This was also not specifically mentioned in the NIS2 proposal. Therefore, the thesis takes a cautious stance on how much the NIS2 Directive will improve cyber and IT resilience among EU member states. As the NIS Directive, the NIS2 Directive also does not take an assertive tone on an international level.

New EU Cybersecurity Strategy

As already mentioned, the European Union has made many new initiatives related to cybersecurity. One of them is the new EU Cybersecurity Strategy which was released in December 2020 and correlates with the NIS Directive and the Critical Entities Resilience Directive. This strategy's two new main priorities are "trust and security at the heart of the EU digital decade," and "cyber and physical resilience of network, information systems and critical entities."[180] The first priority, "trust and security at the heart of the EU digital decade" is significant and different from previous legislation and policy. The reason for this is that the EU plans to take more leadership in terms of cyber resilience, budgetary matters for cybersecurity, and working together with "international partners."[181] This is a rather proactive/assertive move, which the European Union has not done in the past. The EU rather seemed to have a reactive approach to the developments of cyberspace and their threats but did not take proactive leadership. Furthermore, something else that stands out in this priority is that for the first time, the EU mentions the notion of deterrence in "building operational capacity to prevent, deter and respond."[182] In past legislations such as the NIS Directive, the EU did not use the word 'deter,' a term that a more assertive international actor, like the US has used. Does this mean that the European Union is shifting toward being more assertive in terms of cybersecurity? This might be the case since the language and direction of the new cyber strategy is more proactive than previous ones. As for the second priority, "cyber and physical resilience of network, information systems and critical entities," the strategy recognizes the "interconnectedness" of

[180] "New Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," European Commission, Press Corner, 16 Dec 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.
[181] "New Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," European Commission.
[182] "New Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," European Commission.

cyberspace, something many U.S. scholars, like Dr. Harknett speak of and link to the necessity of persistent engagement.[183] The EU's understanding of interconnectedness might not be perceived the same way it is in the U.S., but still suggests that the European Union has more of an idea of the complex nature of cyberspace, which is the first step toward securing it. Overall, the second priority focuses on building more cyber resilience for critical infrastructures, information systems, as well as "the next generation of networks," such as 5G.[184] Recognizing the main vulnerable targets in cyberspace also hints toward the fact that the EU is gaining more knowledge and capacity to somewhat prevent cyber-attacks. The reason the word 'somewhat' is used is because an entity, company, government body etc. will never be able to fully protect itself in cyberspace, however it can attempt to minimize the potential damage of a cyber-attack. Summed up, the New EU Cybersecurity Strategy suggests that the EU is becoming a more proactive actor in cyberspace than it used to be. Whether this necessarily will give the EU more advantages in cyberspace will be discussed later in the thesis.

Further relevant legislation and policies and where the EU is headed in the future

Next to the NIS Directive, the NIS2 Directive and the EU's New Cybersecurity Strategy, further legislation related to cybersecurity in the EU exists that is relevant to mention.

The EU Cybersecurity Act came into force in 2019, is under the umbrella of the European Union's Digital Strategy and is additionally based on the NIS Directive. The legislation recognises as discussed in the interviews, that cybersecurity standards among member states may vary a lot. Therefore, the EU Cybersecurity Act establishes a "certification framework" that "will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures."[185] The certification scheme will apply to "ICT products and services." With the Cybersecurity Act, the EU cybersecurity agency ENISA is also given many more responsibilities and resources to help member states implement a "cybersecurity certification framework," and to support the EU "in case of large-scale cross-border cyberattacks and crises."[186] In the short time that the NIS Directive has been implemented, the EU has evaluated that many cybersecurity gaps exist between member states, which can be seen in the EU Cybersecurity Act. However, as discussed in the conducted

[183] "New Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," European Commission.
[184] "New Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," European Commission.
[185] "The EU cybersecurity certification framework," European Commission, Policies, accessed 7 April 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.
[186] "The EU Cybersecurity Act," European Commission, Policies, accessed 7 April 11, 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

interviews, even with a lot of legislation in place, many gaps still exist between member states in terms of how cybersecurity standards are implemented and whether reliable cybersecurity audits in fact take place. Therefore, only time can tell how much positive effect the Cybersecurity Act 2019 will have on the European Union. As of 2022, cybersecurity experts still see many gaps to be overcome.

With the New EU Cybersecurity Strategy also came a "proposal for a directive on the resilience of critical entities" in December 2020, which will be known as the Critical Entities Resilience (CER) Directive.[187] This Directive will have the purpose of, as the name already tells, providing EU member states with a framework for "ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents."[188] Even though this Directive affects some of the same sectors as the NIS Directive, like banking and energy, the incidents are not solely limited to cyber-attacks, but also include "natural hazards, accidents, terrorism, insider threats, or public health emergencies."[189] However, the CER Directive will still go hand-in hand with the NIS2 Directive. Some of the provisions of the CER Directive will be for member states to "have a strategy for ensuring the resilience of critical entities," "risk assessments" on these critical entities, and a "Critical Entities Resilience Group" for "regular cross-border cooperation."[190] Overall, one can see that the European Union is making large advancements in securing critical infrastructure, a vulnerable target to cyber-attacks.

In 2018, the Council of the European Union additionally updated the EU Cyber Defence Policy Framework which was briefly discussed in the first part of this chapter on the European Union. Initially, this framework had the goal to improve EU member states' "cyber defence capabilities" by offering them special training and education programmes and projects.[191] In the updated version, "priority areas" are added, like "the development of cyber defence capabilities," "the protection of the EU CSDP communication and information networks," "training and exercises," "research and technology," "civil-military cooperation," and

---

[187] "The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU," European Commission, Migration and Home Affairs, 16 Dec 2020, https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en.

[188] "The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU," European Commission.

[189] "The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU," European Commission.

[190] "The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU," European Commission.

[191] "Cyber defence: Council updates policy framework," European Council, Council of the European Union, Press releases, 19 Nov, 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/.

"international cooperation."[192] Within these priorities, certain EU entities are specifically assigned to the priority actions. The 2018 Cyber Defence Policy can be seen as yet another step in the European Union's efforts to improve its cybersecurity and defence capabilities.

It is also important to mention the European Union's 'General Data Protection Regulation' (GDPR), which came into effect in 2018.[193] The regulation has established strict requirements in terms of "data privacy and security" for businesses and organisations within the EU, whether these are EU or non-EU entities. According to the GDPR, it "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data," and "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data," (Art. 1). The GDPR is a significant regulation for the European Union since it is seen as one of the toughest regulations on data privacy and security and highlights the European Union's leadership in this specific area. So, one can conclude from the GDPR that the EU is not just steeping up its leadership in cybersecurity policy, but also in data protection. This again confirms that the European Union is shifting from being a rather reactive/defensive actor toward a more proactive/assertive one.

Finally, the European Union has very recently come to realise that its "institutions, bodies, offices and agencies" need to "bolster their resilience and response capacities against cyber threats and incidents."[194] This is why the EU Commission has proposed a new Cybersecurity Regulation that will improve EU bodies against malicious cyber activities and attacks, in which CERT-EU will have a larger role to play.

Overall, the European Union has not explicitly recognised cyberspace as a strategic space in which actors, including the EU, can gain advantages, however, many other developments have occurred related to cyberspace. First, the most relevant development for the thesis is that the EU has somewhat shifted from being a reactive/defensive actor in cyberspace toward being a more proactive/assertive one. This can be seen in the New EU Cybersecurity Strategy. Second, the EU has become very proactive in drafting various legislation on securing cyberspace and critical entities within the EU itself, but mainly within its member states. Even though there is still room for improvement in implementing cybersecurity standards within member states, and EU institutions, a lot of advancement can be seen compared to the beginning of cybersecurity

---

[192] "Outcome of Proceedings: EU Cyber Defence Policy Framework (2018 Update)," 19 Nov 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf, 8.

[193] "Complete Guide to GDPR compliance," GDPR.EU, accessed 22 April 2022, https://gdpr.eu.

[194] "New rules to boost cybersecurity and information security in EU institutions, bodies, offices and agencies," EU Commission, Press Release, 22 Mar 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1866.

measures within the EU in the early 2000s. The European Union, like the United States, is adjusting its policies and legislation to the complex nature of cyberspace.

The Russian Invasion in Ukraine and its Impact on EU Cybersecurity Policy

Since Russian forces have invaded Ukraine on February 24th, 2022, the European Union has come to terms that it must further strengthen its security and defence policy, including cybersecurity. This can be seen in the outcome of the "Strategic Compass for Security and Defence" meeting which was recently held by the Council of the European Union.[195] One of the main priorities under goal to "secure" was to "further develop the EU Cyber Defence Policy," with the purpose of being "better prepared for" cyber-attacks. [196] Furthermore, the EU will "strengthen the EU Cyber Diplomacy Toolbox," and contribute more toward "the EU's Joint Cyber Unit."[197] The European Union has additionally recognized that Russia will use the domain of cyberspace to attack Ukraine and its Western allies in this war. It has, however, also recognised China, another dominant global actor, as well as other countries, like Afghanistan, as a threat.[198] Further evidence in the "Strategic Compass" also exists that the war in Ukraine has forced the European Union to see cyberspace more as a space in which great powers, state actors and non-state actors operate to gain strategic advantages, and in which the EU must likewise compete. For example, the EU has announced its aim to leverage its cyber capabilities to secure its "access to strategic domains," in which NATO will assist the European Union.[199] This might ultimately shift the EU into a similar mindset as the U.S. in cyberspace, which is more competitive and strategic.

Further statements additionally suggest that the war in Ukraine has forced the European Union to leverage its cybersecurity and defence capabilities. Two months after the invasion in Ukraine had started, the Vice President of the European Commission, Margaritis Schinas, announced that cybersecurity cannot be a "side issue" for the EU, but needs to be a "fundamental pillar" of the Union's "security and economy."[200] He additionally pointed out the need for an actual

[195] Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security," Outcomes of proceedings, 21 March 2022, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.
[196] Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security," 3.
[197] Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security," 22.
[198] Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security," 8-10.
[199] Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security," 23.
[200] European Parliament, "EU preparedness to cyber-attack following Russia invasion on Ukraine: closing statement by Margaritis Schinas, Vice President of the European Commission," Multimedia Centre, 3 May 2022,

"cyber defence capability" and more "resilience," which is why the EU will invest more in securing cyberspace.[201] Something that is also worth mentioning is EU and United States' strengthened cybersecurity cooperation in light of the Russian invasion in Ukraine. In March 2022, the President of the EU Commission, Ursula Von der Leyen, and U.S. President Joe Biden agreed to "advance" their "cooperation on cybersecurity through a variety of actions."[202]

Overall, the war in Ukraine has forced the European Union to seriously consider its defence and security capabilities, which includes cybersecurity. Will this make the European Union see cyberspace as a strategic space and become a more competitive actor, like the United States? As already mentioned, the European Union has already made efforts to improve cybersecurity within the EU before the invasion. However, with the limitations and gaps the EU still faces in securing cyberspace, it is crucial for the EU to move quickly in eliminating those gaps as best as possible.

https://multimedia.europarl.europa.eu/en/video/eu-preparedness-to-cyber-attack-following-russia-invasion-on-ukraine-closing-statement-by-margaritis-schinas-vice-president-of-the-european-commission_I224273.

[201] European Parliament, "EU preparedness to cyber-attack following Russia invasion on Ukraine: closing statement by Margaritis Schinas, Vice President of the European Commission."

[202] European Commission, "Joint Statement by President von der Leyen and President Biden," Statement, 24 March 2022, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_2007.

6. b. 3. Case Study: 'Ghost Writer' Campaign

Like in the chapter of the United States, the thesis will end the discussion of the European Union with a case study, which will be on the hacking campaign 'Ghostwriter.' 'Ghostwriter' has been an active campaign since about 2017 and has mainly targeted Western states and entities, such as the US, NATO, and the European Union. The campaign makes efforts to break "into news websites or social media accounts of government officials in order to publish forged documents, fake news, and misleading opinions meant to sway elections, disrupt local political ecosystems, and create distrust."[203] In the past years, the campaign has increasingly targeted member states, like Latvia, Poland, Lithuania, and institutions of the European Union. In the summer of 2021, 'Ghostwriter' also started targeting German politicians to the point that the European Union warned the campaign not to interfere with the upcoming Bundestag elections in Germany. Germany claimed that the campaign had tried to spread disinformation ahead of the election and that there were signs of recent cyberattacks related to phishing. The European Union suspects that, like in the case of SolarWinds, the attacker behind 'Ghostwriter' is Russia. This is also confirmed by FireEye, who "linked the Ghostwriter campaign to UNC1151, a threat actor that is believed to be backed by the Kremlin."[204] In September 2021, the Council of the European Union released a "Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes," in which it condemned Russia for its "malicious cyber activities," and "urged the Russian Federation to adhere to the norms of responsible state behaviour in cyberspace."[205]

What is interesting in this case and the European Union's statement in regard to Russian malicious cyber activities is how the European Union refers to 'norms of responsible state behaviour in cyberspace.' However, what are these norms, and how do they translate into cyberspace? Can we even identify cyber norms as of now? There are certain norms that are considered in international relations, and which have been written down in, for example, the UN Charter. But, as the world can currently witness with the war in Ukraine, these norms are

---

[203] Catalin Cimpanu "EU formally blames Russia for GhostWriter influence operation," The Record, 24 Sep 2021, https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation/.

[204] Carly Page, "EU warns Russia over 'Ghostwriter' hacking ahead of German elections," TechCrunch, 24 Sep 2021, https://techcrunch.com/2021/09/24/european-council-russia-ghostwriter/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACoi7Hvunl37kwMQEODDu-qvXgXKzeZp7ZOlRgbtUwknuZ4exnmVHdvm-5K6YK0b_qRgbx9Ine8Xekfyls-OFpA8jsBoij5PmvcE7wHeDzJ_YMKQetOcJfDvaoGWRHhtu5cbHfwPeD_JEr0YG06IQ28-PXqaWJXji4okYIPfeMds.

[205] "Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes," European Council, Council of the European Union, 24 September, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/.

often also not respected outside of cyberspace. How can international actors, like the European Union then speak of responsible norms in cyberspace? This case again confirms that cyberspace is a complex space in which traditional norms do not have as much effect. Instead, international actors, like the European Union need to recognise that states and non-state actors will use cyberspace as a space in which they can gain strategic advantage, something the European Union itself needs to adjust to. In the European Union's statement and reaction toward Russian malicious cyber activities, one can also still notice that the EU is still a rather reactive actor and does not make proactive/assertive efforts to 'beat' Russia in cyberspace, or in other words 'be ahead of the game.' This, however, might be the European Union's best chance at securing cyberspace. Additionally, the European Union condemns Russia, but does not deter Russia in an effective manner. In the SolarWinds case, the United States' deterrent reaction with sanctions might have been late, however, some form of deterrence will most likely be more effective than a statement condemning the attacker.

Looking at the New EU Cybersecurity Strategy, which was released in 2020, however, the European Union does take a more proactive leadership role and threatens to deter actors that launch cyber-attacks against the EU. This could not exactly be seen in the EU's reaction toward Russia's undercover cyber operations through 'Ghostwriter,' though. Josep Borrell, the High Representative of the Union for Foreign Affairs and Security Policy, threatened Russia with sanctions but did not follow through with them. This could, however, also be related to the EU's economic ties with Russia. Still, this confirms that, like with the SolarWinds case, deterrence, for example through sanctions, is not always a reliable tool to defend cyberspace on an international level. Especially the European Union needs to adapt to the unique nature of cyberspace in which democratic norms are not always recognised. What the European Union has done, however, is to make renewed efforts to improve European institutions and member states' internal strength and resilience against cyber-attacks. This can be seen in the NIS2 Directive, the CER Directive and the Cybersecurity Act. The European Union has made many legislative attempts to form strong partnerships between governments, agencies, the public and private sectors, which is, as already discussed in the previous case study, the key to eliminating potential vulnerabilities. This also leads to the point that assertiveness and proactiveness need to be not only tied to deterrence and persistent engagement within the government but must be linked to proactive communication and strategy sharing with the private sector and allies of the EU. This is something the EU does well. Overall, the case study shows that the EU is not assertive when it comes to recognising cyberspace as a strategic space in which democratic

norms are less valued but instead is proactive in promoting information sharing, reporting, and regulating cybersecurity norms within the European Union.

6. c. Comparison between the United States and European Union

After a discussion of the United States and European Union cybersecurity policy, strategy and legislation evolvements, the thesis has drawn important elements of comparison. The U.S. and EU cybersecurity developments share both relevant similarities and differences.

Similarities

In terms of similarities, a few points can be made. First, what has become obvious for both the U.S. and the EU is that **cyber policy and strategy are tied to the conditions that the U.S. and the EU both find themselves in**. On the side of the U.S., the discussion revealed that cyber policy and strategy is not as much tied to the current administration that is in place, but rather to what the reality of current cyber threats. As for the EU, this is the same case. Within the EU, relevant legislation and policy has also been shaped due to ongoing threats of cyberspace. This has not been determined by who has had leadership positions within EU institutions. It seems that for both the U.S. and the EU, ongoing legislation and policy has been shaped by the ever-increasing relevance of cyberspace and the national interest in securing it.

Second, both the United States and the European Union **have recently increased their efforts in forming internal/national resilience against potential cyber-attacks and exploitations**. Both international actors have, for example, made it a priority to form strong partnerships between governments and their agencies with the private and public sectors. This includes information sharing, reporting in the case of a cyber-attack and stronger communication in terms of cybersecurity priorities. For the European Union, this can be seen in the initial NIS Directive, but even more so in the NIS2 Directive. Additionally, the EU is currently working on the CER Directive and has formed new regulations, such as the EU Cybersecurity Act. With the Russian invasion in Ukraine, the EU has come to terms that cybersecurity within the Union must be further improved. On the side of the United States, the SolarWinds cyber-attack just recently pushed the state to build more strength against cyber-exploitations. Just after the attack had been detected, the Biden administration released an 'Executive Order on Improving the Nation's Cybersecurity.' The Executive Order in particular focuses on strengthening the government's partnership with the private sector. Before the Biden administration, efforts had already been made to promote a more effective countering of cyber-attacks through the NDAA 2019. Furthermore, the U.S. Senate just recently passed the Strengthening American Cybersecurity Act of 2022, which will require strict reporting in the case of a cybersecurity incident.

Third, the U.S. and EU **recognise the same enemies/competitors in cyberspace**. As was displayed in both case studies, Russia has, become one of the biggest threats to both the EU and the U.S. in cyberspace. Even though the European Union does not specifically mention its competitors in its cybersecurity strategy, as the U.S. does, the EU has still openly condemned Russia for being responsible for 'Ghostwriter' attacks. Furthermore, both the EU and the U.S. see both non-state actors and state actors as competitors in cyberspace. This changed from the 2000s when in particular the U.S. saw terrorists as the main threat. The third point automatically leads to the fourth, which is that the United States and European Union both **recognise one another as allies, striving for international cooperation in securing cyberspace.** This is seen in the White House National Cybersecurity Strategy and Department of Defense Cyber Strategy 2018, as well as the New EU Cybersecurity Strategy. In the White House National Cybersecurity Strategy, Pillar III intends to "Build International Cyber Capability," however, while still maintaining "American influence."[206] In the DoD Cyber Strategy this is similar.[207] The New EU Cybersecurity Strategy also prioritises working together with international allies, but definitely does this with less assertive/proactive intentions of dominating and leading cyberspace on an international level like the U.S., one of the differences that will be mentioned in the next section of the chapter.

The final similarity between the United States and the European Union became clearer after taking a glance at both case studies: Both the U.S. and the EU have proven that **they are equally vulnerable to cyber-attacks and exploitations.** From the cases of SolarWinds and 'Ghostwriter,' one can conclude that both the U.S. and EU are targets in cyberspace and are not capable to fully protect themselves against malicious cyber activities. Both the U.S. and EU still have gaps in securing cyberspace, which can be seen in the ongoing improvements in legislation, national strategy, and policy. However, it seems that after conducting further research, that any entity, institution, or state will never be fully capable of protecting itself in cyberspace. The key is to anticipate the attack before it happens, so that minimum damage is done when the attack does take place.

Differences

Even though the United States and the European Union have several similarities in their cybersecurity strategies, policies, and legislation, some significant differences could be found, too. First, **the European Union has developed more legislation in cybersecurity for the**

[206] "National Cyber Strategy of the United States of America," the Trump White House Archives, 26.
[207] "Summary Department of Defense Cyber Strategy," Department of Defense, 4-6.

digital era than the United States. The European Union has more explicit cybersecurity directives and regulations for EU member states, for example, the NIS and NIS2 Directive, the EU Cybersecurity Act, CER Directive etc. This is also very applicable for data protection and security purposes. The European Union has developed the General Data Protection Regulation, while the United States still struggle with the question of how to regulate data. If the United States and European Union are compared on a more superficial basis, one can say that the U.S. has given states more freedom to delegate their own cybersecurity measures throughout the past, whereas the EU is giving its member states increasingly less freedom in doing so. But it is also important to mention that the United States has recently made more efforts in creating federal cybersecurity laws, which is seen in the Strengthening American Cybersecurity Act of 2022. Overall, the thesis must add that the EU tends to create more regulations than the United States on any issue, though. Cybersecurity is simply one example of this.

Second, **the United States, like its character as an international actor, has a rather more assertive/proactive approach to cyberspace than the European Union.** The United States is very proactive in not just defending cyberspace but being the dominating actor in it. This is different from the European Union. The European Union is not proactive in being the dominating actor in cyberspace and puts a priority on defending cyberspace as best as it can. There is no specific evidence in the conducted research that the European Union aims to be a hegemon in cyberspace, like the United States. A relevant example would be that the United States treats cyberspace more like a military space than the European Union, as seen in the Department of Defense Cybersecurity Strategy. In a military sense, the U.S. uses the notion of deterrence to threaten actors in the case of a cyber-attack. This portrays that the consequences of attacking a military might, like the US will have more disadvantages than advantages for the attacker. This is something the EU has only just started doing in the New EU Cybersecurity Strategy, but in a less aggressive manner than the U.S. Furthermore, the United States' assertive character in cyberspace is seen in its economic efforts to 'be the best,' which is noticeable in Pillar II of the White House National Cyber Strategy 2018. Examples would be to "develop a superior cybersecurity workforce," maintaining "leadership" in the United States' technology and infrastructure, and "maintaining the United States' strategic advantage in cyberspace."[208] It is important to add that the New EU Cybersecurity Strategy shows the European Union has shifted more toward leadership and a proactive attitude in cyberspace than it has in the past years. However, this is still not comparable to the United States. Overall, the United States' more proactive and assertive character in cyberspace also reflects the states' international

[208] "National Cyber Strategy of the United States of America," the Trump White House Archives, 14-17.

character in general. The United States, unlike the European Union, actively pursues to be the global hegemon.

The second point also leads to the third point that **the United States and European Union differ in how they view cyberspace in a strategic and tactical sense.** The United States recognises cyberspace as a space in which non-state actors and state actors, including itself, can gain strategic advantages over other great powers and non-state actors. The perfect example of this would be Stuxnet. Even though the United States never openly admitted its responsibility for the cyber-attack on Iran's nuclear plant, there is much evidence that the U.S. was behind it. The purpose of the attack was most likely linked to gaining a strategic advantage in ongoing negotiations with Iran. Furthermore, the United States as of now uses persistent engagement to maintain its "strategic advantage in cyberspace."[209] The research conducted for the thesis could find no evidence that the European Union uses cyberspace in a strategic way, like the United States does. The EU's legislation and strategy rather focuses on solely protecting and defending cyberspace. Again, the way the United States and the European Union strategically view cyberspace can also lead back to how they act on an international level. The United States overall has the underlying goal to maintain its hegemonic status in the world, especially with the rising might of competitors, such as China and Russia. The European Union, on the other hand, does not implicitly aim or announce to be the world's dominating hegemon. With the ongoing war in Ukraine, however, the European Union might be forced to become a more competitive actor in cyberspace, like the United States.

[209] "National Cyber Strategy of the United States of America," the Trump White House Archives, 16.

7. Summary

In summary, the thesis discussed the cybersecurity and IT strategies of both the United States and the European Union. This was done with the intention of finding out whether a generally assertive international actor, like the United States, necessarily has more advantages in cyberspace than a generally defensive international actor, like the European Union. This will be answered in the conclusion. In the thesis, the term 'assertive actor' is linked to an actor who strives to be proactive and dominant on an international level. A 'defensive actor,' on the other hand, is an actor who rather reacts to the present circumstances and who does what is necessary to protect oneself on an international level, but without the purpose of dominating.

The literature review revealed that the European Union, in fact, is a less assertive actor in cyberspace. It also clarified that the European Union is limited in its cybersecurity strategy, but not whether this had anything to do with its defensive character. Additionally, the European Union's literature on cybersecurity policy is rather based on its timeline, what has legally been passed so far and the gaps and limitations of the EU's cybersecurity policies themselves. On the contrary, US literature portrays international relations theory and the notion of deterrence in cyberspace, something that could not be found in the EU literature. This suggests, as mentioned in the comparison, that the European Union does not see cyberspace as a strategic, or even military space as the United States. It also hints toward United States having dealt with questions of cybersecurity strategy longer and in more depth than the European Union and therefore hints toward the country's more assertive character as an international actor. An actual comparison between the United States and the European Union's cybersecurity policies from an international relations point of view was not found, which is why the thesis takes a rather novel approach.

In terms of United States cyber policy and strategy, the thesis found that the state has significantly shifted in its approach toward cyberspace itself in the past decades. In the 2000s, the U.S., considering the events of 9/11, saw cyberspace as a space of espionage and surveillance in which non-state actors, like criminals and terrorists, were the main enemies or competitors. Especially from 2016/2017 onward, however, the U.S. has started to treat and recognise cyberspace as a tactical space that great powers and non-state actors can use to push their own interests, including U.S. interests. Furthermore, the United States no longer solely relies on deterrence to secure cyberspace: The state also uses 'persistent engagement,' which can be described as 'defending forward.' As for current policy and legislation, the thesis analysed the White House National Cybersecurity Strategy 2018 and the Department of Defense Cybersecurity Strategy 2018, which were both released under the Trump

administration. Both policies confirm that the United States is an assertive international actor in cyberspace, with the DoD Strategy taking a more military approach. The reason these strategies have an assertive character is due to the strategy of persistent engagement, the efforts of being ahead of other great powers from a technological point of view, and the initiative of taking international leadership. After the analysis of these two strategies, the thesis took the current Biden administration into consideration. During the Biden administration, the SolarWinds cyber-attack was detected and revealed, which showcased that the United States was still very vulnerable to malicious cyber activity. More importantly, the attack proves that assertive policy is not the only important factor in securing cyberspace. It is crucial to build internal/domestic resilience, which includes strong partnerships between the government, government agencies, and the public/private sectors. The pursuit of this type of domestic resilience can be seen in Biden's 'New Executive Order on Improving the Nation's Cybersecurity,' as well as the Strengthening American Cybersecurity Act 2022.

When it comes to the European Union, the thesis found that it began to draft cybersecurity policies and legislation later than the United States but has presently drafted many directives and regulations related to cyberspace and the digital era. The European Union is an actor that makes many regulations but does not take the amount of proactive international leadership as the U.S. when it comes to defending cyberspace. This confirms that the European Union is a defensive international actor in cyberspace. This can also be seen in the fact that NATO takes more responsibility in cyberspace from a military and strategic aspect than the EU. As for current cybersecurity policy and legislation, the thesis mainly focused on the NIS Directive, the NIS2 Directive and the New EU Cybersecurity Strategy 2020. While the NIS Directive had many gaps in implementing IT and cybersecurity standards within member states, the NIS Directive intends to close these gaps, whereas it is unclear how effective this will be. The NIS Directive, like Biden's 'New Executive Order on Improving the Nation's Cybersecurity,' is similar in its pursuit of building internal/domestic resilience. In the EU, this includes strong partnerships between the EU, its member states, EU agencies, and the public/private sectors. What was significant in the New EU Cybersecurity Strategy 2020 is that the EU takes a more proactive stance in deterring cyber-attacks and is willing to take more international leadership in this matter. On the other hand, the 'Ghost Writer' case study showed that the EU could at the same time not live up to its intentions of actively deterring malicious cyber activities. This shows that the EU also struggles with securing cyberspace, but additionally from a point of deterring its enemies in a more strategic way. Overall, however, the EU does not lack in legislation for the digital era: Other initiatives that were mentioned in the thesis were the

General Data Protection Regulation, the EU Cybersecurity Act 2019, the CER Directive, the updated EU Cyber Defence Policy Framework 2018, and a new proposal for a Cybersecurity Regulation.

After a discussion of both the U.S. and EU cybersecurity strategies, policies and legislation, the thesis drew the most important similarities and differences between both. In terms of similarities, the U.S. and the EU's cyber policy and strategies are tied to the conditions that the U.S. and the EU both find themselves in, and not to leadership positions. Second, both the United States and the European Union have recently increased their efforts in forming internal/national resilience against potential cyber-attacks and exploitations. Third, the U.S. and EU recognize the same enemies/competitors in cyberspace. Fourth, the United States and European Union both recognize one another as allies, striving for international cooperation in securing cyberspace. And fifth, Both the U.S. and the EU have proven that they are equally vulnerable to cyber-attacks and exploitations. As for differences, the thesis has found that the European Union has developed more legislation in cybersecurity for the digital era than the United States. However, this rather speaks for the EU's role as a heavily regulating force, rather than it being more advanced in securing cyberspace. Second, the United States, like its character as an international actor, has a rather more assertive/proactive approach to cyberspace than the European Union. The European Union is in comparison not proactive in being the dominating actor in cyberspace but puts its priorities on defending cyberspace as best as it can. The third and probably most important point is that the United States and European Union differ in how they view cyberspace in a strategic and tactical sense. The U.S. treats and recognises cyberspace as a tactical space that great powers and non-state actors can use to push their own interests, including U.S. interests. As mentioned in the comparison, the way the United States and the European Union strategically view cyberspace can also be linked to how they act on an international level. The United States overall has the underlying goal to maintain its hegemonic status in the world, especially with the rising might of competitors, such as China and Russia. The European Union, on the other hand, does not implicitly aim or announce to be the world's dominating hegemon.

8. Conclusion

After closely analysing the United States' and European Union's cybersecurity policies, strategies and legislation, the question must be answered whether an assertive international actor, like the U.S., has more advantages in cyberspace than a defensive international actor, like the EU. Considering the results and elements of comparison, the thesis argues that this can be true, but also not true. Due to the United States' assertive/proactive nature in cyberspace and in its policies, it has some advantages. A proactive stance in cybersecurity gives the U.S. more capabilities of anticipating an attack before it has even happened, which is known as 'persistent engagement.' Persistent engagement displays that proactiveness/assertiveness in cyberspace automatically leads to a stronger defence. Furthermore, taking international leadership in cybersecurity can offer the United States more advantages in cyberspace, like driving international cybersecurity initiatives and norms in its own interests. Being an international leader in cyberspace guarantees the United States' interests and therefore security is being defended. Additionally, the thesis recognised that a rather defensive/reactive actor, like the European Union, had disadvantages as it lacked a proactive stance in effectively deterring those who are responsible for malicious cyber activities. This could be seen in the 'Ghostwriter' case study. Here, the European Union could have perhaps benefitted from a more assertive stance against its competitor in cyberspace, Russia.

On the other hand, an assertive international stance does not always guarantee strategic advantages in cyberspace, which can be seen in the SolarWinds case study. SolarWinds and Biden's 'New Executive Order on Improving the Nation's Cybersecurity' displayed that there are many additional factors that contribute toward a successful cybersecurity strategy and policy. One of those important factors is a strong domestic and internal resilience against malicious cyber activities, which entails strong cooperation and communication between the government, its agencies and institutions, and the public and private sectors. Without such cooperation, undetected cyber-attacks are a lot more likely to happen, which was displayed in SolarWinds. More importantly, all entities must know how to proceed and cooperate once such an incident happens. Therefore, the Strengthening American Cybersecurity Act 2022 is crucial new legislation for securing cyberspace in the U.S since it promotes more cooperation and reporting in the case of a cyber-attack. The EU, which is regarded as a defensive/reactive international actor in the thesis, in fact, has proven to be ahead of the United States in creating legislation that ties together private and public sectors with government institutions and establishes reporting systems for malicious cyber activity. This is displayed in the NIS and NIS2 Directive, as well as the EU Cybersecurity Act. This leads to the concluding remark that

just because an international actor is rather defensive/reactive in cybersecurity policy and legislation, this does not mean that the policy/legislation is ineffective.

Apart from answering the research question, the thesis would like to point out something that Dr. Harknett mentioned in the interview and was noticed during the conducted research: Cyber exploitations, hacks, and attacks have over time not exactly turned to be what we once initially expected them to be. Due to the unpredictable nature and outcomes of cyberspace, we often assume that the future will hold large-scale cyber wars, which we have not witnessed up until today. Up until now, cyber exploitations have not lived up to the capacity and expectations we assumed them to be. In the current Ukraine war, for example, mainly conventional weapons are used. This is probably because the process to prepare and launch a cyber-attack takes far more effort than a conventional weapon. This means that cyberspace in a military sense is, in fact, only useful up to a certain threshold. In summary of this, cyberspace indeed comes with many threats, but we must also realise that the likelihood of a full cyberwar is quite slim. The main threat to be considered is attackers/competitors aiming to gain strategic advantage for their own interests, which is mainly done by data theft, unknown hacks, and attacks on critical infrastructure.

9. Bibliography

"About us." CERT-EU. Accessed 01 April, 2022, https://cert.europa.eu/cert/plainedition/en/cert_about.html.

Anagnostakis, Dimitrios. "The European Union-United States cybersecurity relationship: a transatlantic cooperation." *Journal of Cyber Policy* 6. No.2 (April 2021): 1-19. DOI: 10.1080/23738871.2021.1916975.

Carrapico, Helena and André Barrinha. "The EU as a Coherent (Cyber)Security Actor?" *Journal of Common Market Studies* 55. No. 6 (2017): 1254-1272. DOI: 10.1111/jcms.12575.

Cerulus, Laurens. SolarWinds is 'largest' cyberattack ever, Microsoft president says." Politico. February 15, 2021. https://www.politico.eu/article/solarwinds-largest-cyberattack-ever-microsoft-president-brad-smith/

"Challenges to effective EU cybersecurity policy: Briefing Paper." European Court of Auditors. March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

Cimpanu, Catalin. "EU formally blames Russia for GhostWriter influence operation." The Record. 24 Sep 2021, https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation/.

"The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU." European Commission. Migration and Home Affairs. 16 Dec 2020, https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en.

"Complete Guide to GDPR compliance," GDPR.EU, accessed 22 April 2022, https://gdpr.eu.

Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security," Outcomes of proceedings, 21 March 2022, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

Craig, Anthony J.S. and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." *In Realism in Practice*, edited by Davide Orsi, J.R. Avgustin and Max Nurvus, 85-101. Bristol: E-International Relations Publishing, 2018. https://www.e-ir.info/wp-content/uploads/2018/01/Realism-in-Practice-E-IR.pdf#page=100.

Cronk, Terri Moon. "White House Releases First National Cyber Strategy in 15 Years." U.S. Department of Defense. September 21, 2021. https://www.defense.gov/News/News-Stories/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/.

"Cyber defence: Council updates policy framework." European Council, Council of the

European Union. 19 Nov 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/.

"December 17, 2003 Homeland Security Presidential Directive/Hspd-7." The White House President George W. Bush. Dec 17, 2003, https://www.energy.gov/sites/prod/files/HSPD-7.pdf.

"Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes." European Council, Council of the European Union. 24 September, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/.

"Definition of Cybersecurity – Gaps and overlaps in standardization." ENISA European Union Agency for Cybersecurity. Publications. July 1, 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

"Department of Defense Strategy for Operating in Cyberspace." Department of Defense. July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

"Details of Treaty No. 185." Council of Europe Portal. Treaty Office. Accessed 29 March 2022, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Edegbeme-Beláz, Annamária. "The changing role of the EU in cybersecurity." *Legal and strategical aspects of information and cyber security* (2019): 17-30. https://www.researchgate.net/publication/334173763_The_changing_role_of_the_EU_in_cybersecurity

EEAS Homage. "EU imposes first ever cyber sanctions to protect itself from cyber-attacks." The Common Security and Defence Policy (CSDP). July 30, 2020. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/83572/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en.

ENISA: European Union Agency for Cybersecurity. "NIS Directive." Details. Accessed January 2, 2022. https://www.enisa.europa.eu/topics/nis-directive.

"The EU Cybersecurity Act." European Commission. Policies. Accessed 7 April 11, 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

"The EU cybersecurity certification framework." European Commission. Policies. Accessed 7 April 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

European Commission, "Joint Statement by President von der Leyen and President Biden," Statement, 24 March 2022, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_2007.

European Parliament, "EU preparedness to cyber-attack following Russia invasion on

Ukraine: closing statement by Margaritis Schinas, Vice President of the European Commission," Multimedia Centre, 3 May 2022, https://multimedia.europarl.europa.eu/en/video/eu-preparedness-to-cyber-attack-following-russia-invasion-on-ukraine-closing-statement-by-margaritis-schinas-vice-president-of-the-european-commission_I224273.

EUR-Lex. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." Document 32016L1148. July 6, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

EUR-Lex. "Directive of the European Parliament and of the Council." Document 52020PC0823. December 12, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN.

"Executive Order – Commission on Enhancing National Cybersecurity." the White House President Barack Obama. Office of the Press Secretary. Feb 09, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

"Executive Order – Promoting Private Sector Cybersecurity Information Sharing." the White House President Barack Obama, Office of the Press Secretary. Feb 13, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

"FACT SHEET: Cyber Threat Intelligence Integration Center." the White House President Barack Obama. Office of the Press Secretary. Feb 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

Fischerkeller, Michael P. and Richard J. Harknett. "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*." Lawfare* (November 2018). https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

Friedman, Allan and P.W. Singer. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press, 2014.

Fung, Brian. "Biden administration says investigation into SolarWinds hack is likely to take 'several months.'" CNN Politics. Feb 17, 2021, https://edition.cnn.com/2021/02/17/politics/solarwinds-hack-investigation/index.html.

Geers, Kenneth. "Alliance Power for Cybersecurity." Atlantic Council. 2020. https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Alliance-Power-for-Cybersecurity_Geers.pdf

Harknett, Richard J. "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few." *Contemporary Security Policy* 24(1) (2003): 13-45. DOI: 10.1080/13523260312331271809

Harknett, Richard. "United States Cyber Command's New Vision: What it Entails and Why it

Matters." *Lawfare* (March 2018). https://lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters.

Harknett, Richard. "U.S. Cybersecurity Policy." Interview by Lara Siebrecht. March 3, 2022.

Herman, Arthur. "A National Cybersecurity Strategy: Better Late Than Never." Forbes. September 24, 2018. https://www.forbes.com/sites/arthurherman/2018/09/24/a-national-cybersecurity-strategy-better-late-than-never/?sh=d29dcf42a2a5.

"H.R. 145 – Computer Security Act of 1987." Congress.Gov. Accessed 17 March 2022. https://www.congress.gov/bill/100th-congress/house-bill/145.

Jibilian, Isabella and Katie Canales. "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. April 15, 2021. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Karahan, Saltuk, Hongyi Wu and Leigh Armistead. "Evolution of US Cybersecurity Strategy." In *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, edited by Noëlle van der Waag-Cowling and Louise Leenen, 168-176. Stellenbosch: ACPI, 2019.https://books.google.at/books?hl=en&lr=&id=UfedDwAAQBAJ&oi=fnd&pg=PA168&dq=us+cybersecurity+strategy&ots=CZDC6KsRd4&sig=muvUKODZFvh5fXGCx2PnIefAp9c&redir_esc=y#v=onepage&q=us%20cybersecurity%20strategy&f=false.

Killeen, Molly. "EU demands end to Russian-linked cyberattacks ahead of German elections." Euractiv. September 24, 2021. https://www.euractiv.com/section/cybersecurity/news/eu-demands-end-to-russian-linked-cyberattacks-ahead-of-german-elections/.

Lewis, James Andrew. "Federal Cybersecurity Initiatives Timeline: Draft 1.b." Center for Strategic & International Studies. May 9, 2016, https://www.csis.org/blogs/strategic-technologies-blog/federal-cybersecurity-initiatives-timeline.

Lobell, Steven E. "Structural Realism/Offensive and Defensive Realism." *International Studies: International Study Association and Oxford University Press.* (December 2017): https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304, 1-25.

Markopoulou, Dimitra, Vagelis Papakonstantinou and Paul de Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation." *Computer Law & Security Review* 35. Issue. 6 (November 2019): 1-11. https://doi.org/10.1016/j.clsr.2019.06.007.

Marmor, Andrei. "Legal Positivism: Still Descriptive and Morally Neutral." *Oxford Journal of Legal Studies.* Vol. 26. No. 4 (2006), 683-704.

McGuiness, Damien. "How a cyber attack transformed Estonia." BBC News. 27 April 2017,

https://www.bbc.com/news/39655415.

"Memorandum For Secretaries of the Military Departments: Establishment of a Subordinate Unified U.S. Strategic Command for Military Cyberspace Operations." The Secretary of Defense. Jun 23, 2009, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf.

Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*, 5th ed., revised, (New York: Alfred A. Knopf, 1978), pp. 4-15. https://www.mtholyoke.edu/acad/intrel/morg6.htm.

"Moving IT forward." SolarWinds. Accessed April 5, https://www.solarwinds.com/homepage-3c?adobe_mc_sdid=SDID%3D3E840169ABD6542B-633360A32EB97B8B%7CMCORGID%3D8D6867C25245AEFB0A490D4C%40AdobeOrg%7CTS%3D1649333489&adobe_mc_ref=https%3A%2F%2Fwww.google.com

Naake, Lutz. "Cybersecurity in the German Private Sector." Interview by Lara Siebrecht. 25 Mar, 2022.

"National Cyber Incident Response Plan. Interim Version." Department of Homeland Security. September 2010, https://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf.

"National Cyber Strategy of the United States of America." The Trump White House Archives. September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"National Security Presidential Directives (NSPD) George W. Bush Administration." Federation of American Scientists: Intelligence Resource Program. Accessed 18 March 2022, https://irp.fas.org/offdocs/nspd/index.html.

"National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23." The White House Washington. Jan 8, 2008, https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

"The National Strategy to Secure Cyberspace." The White House Washington. Feb 2003, https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf.

"New Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient." European Commission. Press Corner. 16 Dec 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

"New rules to boost cybersecurity and information security in EU institutions, bodies, offices and agencies." EU Commission. Press Release. 22 March 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1866.

"NIS-Directive." ENISA European Union Agency for Cybersecurity. Topics. Accessed 28 March 2022, https://www.enisa.europa.eu/topics/nis-directive.

"NIST Releases Cybersecurity Framework Version 1.0." NIST. Feb 12, 2014,

https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10.

"The NIS2 Directive: A high common level of cybersecurity in the EU." Briefing. EU Legislation in Progress. Dec 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

"The NIS2 Directive: A high common level of cybersecurity in the EU." European Parliament Think Tank. Briefing. 01 Dec 2021, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

Nye, Joseph S. Jr. "Deterrence and Dissuasion in Cyberspace." *International Security*. 41(3). 44-71. https://doi.org/10.1162/ISEC_a_00266.

"One vendor. One platform. One single pane of glass." SolarWinds. Orion Products. Accessed 5 April 2022, https://www.solarwinds.com/solutions/orion.

"Outcome of Proceedings: EU Cyber Defence Policy Framework." Council of the European Union. 18 Nov 2014, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf.

"Outcome of Proceedings: EU Cyber Defence Policy Framework (2018 Update)." 19 Nov 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf.

Page, Carly. "EU warns Russia over 'Ghostwriter' hacking ahead of German elections." TechCrunch. 24 Sep 2021, https://techcrunch.com/2021/09/24/european-council-russia-ghostwriter/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACoi7Hvunl37kwMQEODDu-qvXgXKzeZp7ZOlRgbtUwknuZ4exnmVHdvm-5K6YK0b_qRgbx9Ine8Xekfyls-OFpA8jsBoij5PmvcE7wHeDzJ_YMKQetOcJfDvaoGWRHhtu5cbHfwPeD_JEr0YG06IQ28-PXqaWJXji4okYIPfeMds.

"Protection of National Security and Public Safety Act." House of Representatives. July 23, 1999, https://www.congress.gov/106/crpt/hrpt117/CRPT-106hrpt117-pt4.pdf.

"Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center." Department of Homeland Security. Oct 30, 2009, https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened.

Schwartz, Samantha. "One year later: has SolarWinds changed how industry builds software?" Cybersecurity Dive. Dec 14, 2021, https://www.cybersecuritydive.com/news/solarwinds-1-year-later-cyber-attack-orion/610990/.

Sliwinski, Krzysztof Feliks. "Moving beyond the European Union's Weakness as a Cybersecurity Agent." *Contemporary Security Policy* (September 2014): 1-19. http://dx.doi.org/10.1080/13523260.2014.959261.

"Special Report. Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats." European Court of Auditors. 2022, https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_EN.pdf.

"Summary Department of Defense Cyber Strategy." Department of Defense. 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

The White House. "Executive Order on Improving the Nation's Cybersecurity." Briefing Room, Presidential Actions, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Think Tank European Parliament. "The NIS2 Directive: A high common level of cybersecurity in the EU." Briefing. December 1, 2021. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

Trump White House Archives. "National Cyber Strategy of the United States of America." September 2018, https://trumpwhitehouse.archives.gov/wpcontent/uploads/2018/09/National-Cyber-Strategy.pdf.

"US-CERT. United States Computer Emergency Readiness Team." Homeland Security. Accessed 18 March 2022, https://www.cisa.gov/uscert/sites/default/files/publications/infosheet_US-CERT_v2.pdf.

U.S. Department of Defense. "Summary: Department of Defense Cyber Strategy." 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

"U.S. Senate Unanimously Passes Cybersecurity Legislation Requiring 72 Hour Cyber Incident Notification." The National Law Review. Volume XII. Number 100. April 10, 2022, https://www.natlawreview.com/article/us-senate-unanimously-passes-cybersecurity-legislation-requiring-72-hour-cyber.

Walsh, Joe. "Here Are Some Of The Major Hacks The U.S. Blamed On Russia In The Last Year." Forbes. June 1, 2021. https://www.forbes.com/sites/joewalsh/2021/06/01/here-are-some-of-the-major-hacks-the-us-blamed-on-russia-in-the-last-year/?sh=3771cfc05b9e.

Wang, Faye F. "Legislative Developments in Cybersecurity in the EU." *Amicus Curiae: The Journal of the Society for Advanced Legal Studies* 1. No. 2 (2020): 233-259. https://doi.org/10.14296/ac.v1i2.5131.

Watanabe, Seiko. "States' Capacity Building for Cybersecurity: An IR Approach." *Human-Centric Computing in a Data-Driven Society*. Pp. 222-232.

"What is Cybersecurity?" Cybersecurity & Infrastructure Security Agency. Last modified

Nov 14, 2019, https://www.cisa.gov/uscert/ncas/tips/ST04-001.

Willett, Marcus. "Lessons of the SolarWinds Hack." *Global Politics and Strategy.* Vol. 63. Issue 2. 30 March 2021, https://www.tandfonline.com/doi/full/10.1080/00396338.2021.1906001, pp 7-26.

Zacherl, Bernard. "Cybersecurity in the Austrian Private Sector." Interview by Lara Siebrecht. 11 Mar, 2022.

"2007 cyber attacks on Estonia." Stratcomcoe. 2007, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

10. Appendix

10. a. Interview with Dr. Professor Harknett from the University of Cincinatti, conducted by Lara Siebrecht on March 2nd 2022 – "U.S. Cybersecurity Policy"

1. How has the United States Cybersecurity strategy shifted over the past years in the United States? How has it changed from administration to administration?

Harknett claims that shifts are not tied to an administration, but shifts are rather tied to the conditions in cyberspace and the security that the US finds itself in. Initially, the US saw large scale cyber-attacks and attacks against critical infrastructure as a threat and spoke of "attacks of significant consequence." Furthermore, the US was heavily influenced by the 9/11 attack and therefore mainly saw criminals and terrorists as the enemy in cyberspace.

The professor also mentions that US policy from the early 2000s until 2015 focused mainly on law enforcement in cyberspace and criminals in cyberspace. Here, deterrence was the dominant mechanism in US planning. Even though the US stated in 2015 that deterrence would be used as a response strategy, its cyber policy would be constrained, and that the US would be careful about using cyber, this was obviously not the case which could be seen in Stuxnet. Even though the US never publicly admitted its association with Stuxnet, from a US point of view, the cyberattack could have been launched to leverage negotiations with the Iranians.

After 2015, Dr. Harknett explains that the operational space in cyber shifts within the United States. This is especially the case when the US realizes that it is losing its ground to different actors in cyber. Unlike the previous strategies, the US from 2016 onward does not treat cyber as a space of war or single attacks but acknowledges that in cyberspace operations are linked to achieving a larger goal. This is what Harknett refers to as a "campaign." Campaigns are more likely to occur in cyberspace than in an isolated attack. The US slowly shifts from 2016 onward from a response force to a persistent force in cyberspace, which Harknett sees as a critical moment for US cybersecurity strategy.

In 2017, the Department of Defense also realizes that great powers are using cyberspace below the threshold of war for strategic interests, which can also be seen in the National Security Strategy of 2017 and the 2018 Department of Defense and White House National Cyber Security Strategies. Harknett emphasizes that for the first time, cyberspace is seen as a strategic and tactical space. Before that, it was seen more as a domain of sabotage, espionage, and surveillance. The United States also recognizes that deterrence may be effective, but persistent engagement is the way forward in cyberspace. Persistent engagement is the way to deal with deterrence competitively in cyberspace.

Again, Dr. Harknett emphasizes why the United States' strategy of persistent engagement is important. Persistent engagement means that you are "defending forward:" There is a temporal element to it since a persistent actor is anticipating the exploitation before it has been exploited. It is also required to be in other networks than the own one. To defend, one needs to be ahead of the potential attack. If the actor can anticipate, it can create anticipatory resilience before the attack occurs. Harknett mentions the example of the press. Before the acknowledgement of persistent engagement, the Department of Defense and other US agencies would hide potential cyber-attacks from the press. Now, however, the US Cyber Command is public, for example on the "Virus Total" website that is used to share malware information and threats. The US also granted the FBI authorization to help small companies

with cyber vulnerabilities in the case of a threat and works closely with the private sector to prevent exploitation before it happens.

From a legal perspective, Harknett explains that a major change in US legislation was the 2019 US National Defense Authorization Act 2019 (NDAA). The NDAA authorized the commander of US cyber command to move more rapidly when an opportunity would arise for the US to exploit for its defence. In the PPD 20 (Presidential Directive 20) under the Obama administration, cyber operations were still treated like nuclear operations where the authorization had to come directly from the president. For example, the FBI would never have had the power they have now in the old strategy. The additional new authorization, the NSPN 13, gave more authorities down to the operational level, also in Congress.

Lastly, Dr. Harknett adds that some representatives of the US government still find it hard to accept persistent engagement since it is hard to break a paradigm.

2. Questions 2 and 3 will be on the most recent National Cybersecurity Strategy from 2018 under the Trump administration:
The cybersecurity strategy mentions the notion of deterrence and the balance of power. As an international relations scholar, would you consider this an appropriate approach toward cyberspace?

Dr. Harknett explains that deterrence is still valid, but it applies to specific conditions, for example for nuclear terms. In cyberspace, this needs to be leveraged. The 2018 cyber strategy, however, recognizes great powers as competitive actors in cyberspace who want to undermine the United States. Therefore, the notion of deterrence is valid. But the US also recognizes that cyberspace is a new scene of competition, in which one can gain strategically without going to war.

On a side not, Dr. Harnett mentions that the United Kingdom also mentions the words “persistent” and “assertive” in their National Cyber Force in March 2021. The interviewer, therefore, recognizes that persistent engagement is also being acknowledged outside of the US.

3. The cybersecurity strategy also mentions “persistent engagement,” which you refer to in your work and research. What makes cyber so different from traditional military approaches? And what are the norms in this space?

Dr. Harknett explains that what makes cyberspace so different is its structural interconnectedness. In Cyberspace, every actor is in constant contact, which means that another actor in cyberspace will always have the capacity to exploit you. This might not happen in one attack but can cumulatively over time have a big impact. Furthermore, benign actors, the private sector, allies, adversaries, and non-state actors can be as powerful as a state in cyber. The individual also has gained more power in this domain, which is very different from traditional military approaches.

Furthermore, he explains that the combination of scales, scope, and speed is what makes cyberspace so different and unpredictable. In a realm of constant contact, an individual actor can make significant impacts with the scale, scope and speed of cyberspace! This is an enormous shift in military relative power. An example Harknett mentioned was how North Korea was almost able to perform a bank theft of about 1 billion US dollars in the Bangladesh national bank. This would have been a lot more difficult with traditional military means.

3. Would you consider the United States' cybersecurity strategy more assertive/proactive, or defensive/reactive? What is better in your opinion?

Dr. Harknett states that just because an actor in cyberspace is active and assertive, this does not mean that the actor cannot be defensive at the same time. To him, assertiveness simultaneously means improving defense capabilities in cyberspace. In cyberspace, taking initiative is better for the defence, too. He explains that security is found in the initiative and sustaining the initiative. Security lies in seizing and maintaining and exploiting before an attack takes place.

As for the US, Dr. Harknett sees it as primarily assertive, especially with the new cyber security strategy in place.

4. Do you see the United States engaging in a cyberwar in the near future, especially with the war that has escalated between Ukraine and Russia?

Dr. Harknett does not think that there will be a great power war without cyber operations. Alone the US does not operate without being connected to a network. However, as one can see in the ongoing war in Ukraine, cyber can be a part of war, but we should also not overplay it. For example, Russia has sent a missile to take out a TV tower in Ukraine. This could have probably also been done through a cyber-attack. Here, Harknett emphasizes that sending a missile, for example, is a lot easier than preparing and launching an effective cyber-attack. However, cyber can be effectively used while conventional military attacks are taking place as a distraction.

Harknett finally gives three reasons why no obvious Russian cyber-attack could be seen in Ukraine up until now: First, Ukrainians could have a better cyber defense than expected. Second, Russia might not need to integrate its cyber capabilities at the moment and might be holding them in reserve for when they are needed. Third, Russia may not be using its cyber capabilities because it does not want to give them away to the US and NATO at this point in time.

10. b. Interview with Bernard Zacherl from Ernst and Young Austria, conducted by Lara Siebrecht on March 11th 2022 – "Cybersecurity in the Austrian Private Sector"

Original Version:

1.Die NIS Richtlinie wird als erste offizielle Richtlinie im Thema Cybersicherheit in der EU angesehen. Können Sie erklären, wie diese Richtlinie im privaten Sektor adoptiert wurde und wie Sie Firmen dabei geholfen haben sich an das neue Gesetz zu richten?

Herr Zacherl erklärt, dass die Überführung der NIS Richtlinie vor 3 Jahren zustande gekommen ist, jedoch hat sich seiner Meinung nach wenig getan und der Prozess war eher „schleppend." Das liegt daran, dass es nicht effektive Sanktionen bei dieser Richtlinie gibt, wie zum Beispiel bei dem GDPR Gesetz. Die Überführung des NIS Gesetzes war aus diesem Grund nicht wie ursprünglich erhofft. Herr Zacherl erklärt, wie EU-Mitgliedsstaaten selbst die Entscheidung treffen konnten, welche Firmen von der Richtlinie betroffen wären. Deswegen gab es auch einen großen Unterschied bei EU-Ländern, wie viele Firmen sich an das Gesetz gerichtet haben. Ein massiver Unterschied ist zum Beispiel zwischen Ungarn und Finnland zu sehen: In Ungarn waren nach der NIS I Richtlinie 250 Firmen betroffen, wobei es in Finnland 4000 waren. In Österreich schätzt Herr Zacherl, dass ungefähr 400 Firmen betroffen waren. Zusätzlich sagt Herr Zacherl, dass die EU-Mitgliedsstaaten Deutschland und Frankreich strenger umsetzen als die meisten anderen Mitgliedsstaaten. Generell hatten Mitgliedsstaaten auch die Freiheit darin zu entscheiden, welche Sektoren von der Richtlinie betroffen waren. In Österreich wurden zum Beispiel Bankwesen ausgenommen, wobei der Energiesektor sehr relevant für die Richtlinie in Österreich ist. In Österreich selbst hat man sich zusätzlich an die ISO-27001 Zertifizierung und an „best practices" der NIS Richtlinie gerichtet.

2. Sahen Sie bei der NIS I Richtlinie Einschränkungen? Worauf hoffen Sie in der NIS 2 Richtlinie?

Herr Zacherl erwähnt, dass es notwendig ist, etwas zu ändern und dass die erste Version der NIS 2 Richtlinie Ende 2021 erschienen ist. Jedoch variiert es sich wieder von Staat zu Staat, wie wichtig das genommen wird. Bei Frankreich zum Beispiel steht die NIS 2 Richtlinie weit oben auf der Agenda. Inhaltlich wird die Richtlinie gleichbleiben, jedoch wird diesmal die EU selbst entscheiden, welche Unternehmen betroffen sind und welche nicht. Herr Zacherl deutet darauf hin, dass die Zahl der betroffenen Unternehmen in Österreich sich verdreifachen wird. Bei den betroffenen Firmen unterscheidet man zwischen kritischen und wichtigen Unternehmen. Oft kommt die Selektion auf die Größe, den Umsatz und die Branche der Firma in Frage. Kritische Unternehmen brauchen eine Zertifizierung und wichtige Unternehmen werden nur im Anlassfall geprüft. Jedoch haben beide Arten von Firmen eine Meldepflicht.

3. Was ist die ISO-27001 Zertifizierung?

Die ISO-27001 Zertifizierung kommt von der Non-Profit Organisation „International Organization for Standardization." Die Organisation stellt unterschiedliche „best practice" Standards zur Verfügung, die eigentlich immer analog aufgebaut sind und unterschiedliche Schritte und Anforderungen zur Verfügung stellen, um eine lokale Zertifizierung zu erhalten. Eine Serie davon ist die ISO-27001 Zertifizierung, mit der auch EY arbeitet.

4. Was sind ihrer Meinung nach die größten Herausforderungen Cybersicherheit Standards bei Firmen einzurichten?

Bei NIS relevanten Unternehmen ist die größte Hürde bereits aufgrund der definierten Zuteilung des Unternehmens überwunden. Bei den Unternehmen, die nicht NIS relevant sind, lautet die Frage, was eigentlich zertifiziert werden sollte. Hier wird oft ein Risk Assessment gemacht. Jedoch, ist hier wieder die Frage, was genau bewertet wird. Herr Zacherl fragt sich zum Beispiel oft, was für Dokumente der Firma überhaupt bewertet werden sollten.

5. Gelten die gleichen Herausforderungen in Cybersicherheit im öffentlichen Sektor? Oder sind diese zum Teil anders?

Herr Zacherl sagt, dass sich im öffentlichen Sektor sehr viel tut. Je näher ein öffentliches Institut jedoch zum Staat ist, desto weniger Verplichtungen hat es, etwas im Thema Cybersicherheit selbst zu tun. Das liegt daran, dass der Staat seine Cybersicherheitsstandards selbst bestimmt. Beispiele wären Krankenhäuser, Energiekonzerne und Straßenbau.

6. Wie schaut die Implementierung von Cybersicherheitsprogrammen aus? Kann es jemals perfekt sein?

Herr Zacherl bestätigt, dass es niemals perfekt sein kann. Es wird immer Lücken in Cybersicherheitsprogrammen geben, da sie von Menschen betrieben werden und sie sehr Prozess lästig sind. Hierbei sind auch alle Sektoren betroffen, jedoch gibt er zu, dass vor allem Bankwesen sehr stark reguliert sind. Ihm fällt auf, dass vermehrt Angriffe in Operational Technology (OT) erscheint und wo Geld das Angriffsziel ist. Beispiele von Cyberattacken wären hier der Ölpipeline Angriff bei OMV und der Angriff auf SalzburgMilch GmbH.

7. Diese Frage gilt nur, wenn Sie mehr von US-Cybersicherheit Richtlinien wissen. Wenn ja, wie würden Sie diese zu Österreich oder der EU vergleichen?

Herr Zacherl erwähnt, dass er nicht sehr viel Erfahrung mit US-Richtlinien hat. Jedoch kann er sagen, dass die USA technisch keine Vorteile gegenüber der EU hat. Was Cybersicherheit angeht, denkt er, dass der Ansatz und Umsatz wahrscheinlich schneller sind, was vielleicht die USA ein paar mehr Vorteile gibt, jedoch nicht viele. Den Ansatz selbst sieht er in den USA als reaktiv auf was sich im Markt bewegt.

Translated Version:

1. The NIS Directive is considered the first official cybersecurity directive in the EU. Can you explain how this directive was adopted in the private sector and how you helped companies to comply with the new law?

Mr Zacherl explains that the transition of the NIS Directive took place about 3 years ago, however, in his opinion, little has happened, and the process has been rather "slow." There are no effective sanctions with this directive, such as with the GDPR law. For this reason, the transition of the NIS law was not as originally hoped.
Mr Zacherl explains how EU member states could decide for themselves which companies would be affected by the directive. That is why there was a big difference among EU member states in how many companies complied with the law. A massive difference can be seen, for example, between Hungary and Finland: In Hungary, 250 companies were affected by the NIS I Directive, whereas in Finland there were 4000 that were affected. In Austria, Mr Zacherl estimates that about 400 companies were affected. Additionally, Mr Zacherl says that the EU member states Germany and France have implemented the NIS Directive more strictly than most other member states. Generally, member states also had the freedom to decide which

sectors were affected by the directive. In Austria, for example, banking was exempted, while the energy sector is very relevant to the directive. In Austria itself, the ISO 27001 certification and best practices of the NIS Directive were also taken into account.

2. Did you see any limitations in the NIS I directive? What are you hoping for in the NIS 2 guideline**?**

Mr Zacherl mentions that there is a need to change something and that the first version of the NIS 2 directive was released at the end of 2021. However, it again varies from country to country how this is adopted. In France, for example, the NIS 2 directive is high on the agenda. In terms of content, the directive will remain the same, but this time the EU itself will decide which companies are affected and which are not. Mr Zacherl indicates that the number of affected companies in Austria will triple. Among the affected companies, a distinction is made between critical and important companies. Often the selection is based on the size, the turnover and the industry of the company. Critical companies need certification and important companies are only audited in case of an occasion. However, both types of companies have a reporting obligation.

3. What is the ISO-27001 certification?

The ISO-27001 certification comes from the non-profit organization "International Organization for Standardization." The organization provides different "best practice" standards, which are always analogous in their structure and provide different steps and requirements to obtain local certification. One series of these is ISO-27001 certification, which EY also works with.

4. In your opinion, what are the biggest challenges in setting up cybersecurity standards at companies?

For NIS relevant companies, the biggest hurdle is already overcome due to the assignment of the company. For non-NIS relevant companies, the question is what should be certified. Here, a risk assessment is often done. However, here the question remains what exactly should be assessed. Mr Zacherl, often wonders, for example, what documents of the company should be assessed.

5. Do the same cybersecurity challenges apply in the public sector? Or are some of these different?

Mr Zacherl says that a lot is happening in the public sector. However, the closer a public institution is to the state, the fewer obligations it has in cybersecurity itself. This is because the state determines its own cybersecurity standards. Examples would be hospitals, energy companies, and road construction.

6. What does cybersecurity implementation look like? Can it ever be perfect?

Mr Zacherl confirms that it can never be perfect. There will always be gaps in cybersecurity programmes because they are run by humans and they take a long time to process. In this regard, all sectors are affected, but he admits that banking, in particular, is heavily regulated. He notices that more attacks are appearing in Operational Technology (OT) and where money is the target. Examples of cyberattacks are the oil pipeline attack at OMV and the attack on SalzburgMilch GmbH.

7. This question only applies if you know more about US cybersecurity policies. If so, how would you compare them to Austria or the EU?

Mr Zacherl mentions that he does not have much experience with US policies. However, he can say that from a technical aspect the US has no advantages over the EU. Regarding cybersecurity, he thinks that the approach and turnover in the US are probably faster, which maybe gives the US a few more advantages, but not many. He thinks that the approach itself in the US is reactive to what is going on in the market.

10. c. Interview with Lutz Naake from Ernst and Young Germany, conducted by Lara Siebrecht on March 25th 2022 – "Cybersecurity in the German Private Sector"

Original Version:

1. Die NIS Richtlinie wird als erste offizielle Richtlinie im Thema Cybersicherheit in der EU angesehen. Können Sie mir erklären, wie diese Richtlinie in deutschen kritischen Infrastrukturen adoptiert wurde und die KRISTIS Regulierung ergänzt hat?

Herr Nakke erklärt, dass die NIS Richlinie das Rahmenwerk der EU für Informationssicherheit ist. Er fügt hinzu, dass es einen Unterschied zwischen Cybersicherheit und Informations- (IT) Sicherheit gibt. Bei Cybersicherheit handelt es sich um Angriffe von außen und bei Informationssicherheit kommen die meisten Ausfälle beim Changemanagement zustande. In den meisten Fällen geht es bei der NIS Richtlinie um IT-Sicherheit. Herr Naake erklärt, dass Deutschland bereits in 2015 ein eigenes IT-Sicherheitsgesetz veröffentlicht hat bevor die NIS Richtlinie in 2016 verordnet wurde. Er betont hier, dass die NIS Richtlinie tatsächlich nur ein Rahmenwerk ist, da es sich um eine Richtlinie handelt. Herr Naake beschäftigt sich mit sogenannten KRITIS Sektoren (Kritische Sektoren), wie beispielsweise Krankenhäuser. Verschiedene KRITIS Sektoren haben verschiedene Schwellenwerte, die man beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren muss. Der Schwellenwert bei Krankhäusern liegt zum Beispiel bei 30.000. Nach der Registrierung des Schwellenwerts wird schließlich die passende Technik zur IT-Sicherheit implementiert. Herr Naake rät mir, die Open KRITIS Seite anzusehen. Etwas, dass einzigartig in Deutschland ist, ist die Pflicht alle zwei Jahre auditiert werden zu müssen. Bei diesem Prozess kommt eine externe Person zum Unternehmen und prüft, ob die geforderten IT-Sicherheitsstandards tatsächlich umgesetzt werden.

2. Was für Einschränkungen sahen Sie in der NIS Richtlinie? Worauf hoffen Sie in der NIS 2 Richtlinie?

Herr Naake sagt, die NIS 1 Richtlinie wäre zu wage und grob. Die lokalen Gesetze haben sich sehr unterschieden, zum Besipiel in IT-Sicherheitsverpflichtungen, aber auch in den betroffenen kritischen Infrastrukturen. Da Deutschland pflichtmäßig Audits durchführt, werden automatisch die IT-Sicherheitsstandards umgesetzt. Das ist nicht der Fall in den meisten EU-Mitgliedsstaaten. Österreich richtet sich seit 2015 teilweise an Deutschland was IT-Sicherheit angeht, jedoch gibt es in Deutschland noch mehr Anforderungen. Bei der NIS 2 Richtlinie erhofft sich Herr Naake mehr Audit Verplichtungen, was jedoch wahrscheinlich nicht der Fall sein wird. Etwas, dass sich jedoch verbessern wird in die Konkretisierung betroffener Unternehmen in der NIS 2 Richtlinie.

3. Können Sie mir mehr über das KRITIS IT-Gesetz sagen? Was ist der Unterschied zum IT-Sicherheitsgesetz?

Herr Naake erklärt, dass das KRITIS IT-Gesetz seit 2017 existiert und Schwellenwerte, sowie Sektoren bei der IT-Sicherheit kritischer Infrastrukturen zuordnet. Seit 2018 führt Herr Naake anhand dieses Gesetzes Prüfungen und Audits mit seinem Team durch. Eine zusätzliche Aufgabe für ihn ist es, Transformationen bei Unternehmen durchzuführen, um das KRITIS Gesetz umzusetzen. Er erklärt zusätzlich, dass das Institut der Wirtschaftsprüfer in Deutschland (IDW) mit der Unterstützung vom BSI einen Anforderungskatalog zur Konkretisierung von KRITIS erstellt hat. Das IT-Sicherheitsgesetz wurde im Jahr 2015 veröffentlicht und ist das Rahmenwerk für IT-Sicherheit in Deutschland. Jedoch hängen beide Gesetze zusammen.

4. Was sind ihrer Meinung nach die größten Herausforderungen IT-Sicherheitsstandards bei Firmen und kritischen Infrastrukturen einzurichten?

Herr Naake sieht insbesondere bei der Produktions IT (OT) Herausforderungen. Das ist der Fall, da bei OT vieles von Maschinen gesteuert wird und diese zum Teil noch alte Betriebssysteme haben. Die Gefahr bei OT Betriebssystemen ist oft Ransomware, ein Wurm, der das Firmensoftware eindringt. Was Herr Naake auch als Herausforderung sieht ist das Notfallmanagement bei einem IT-/Cyber-Angriff. Vielen Unternehmen fällt es schwer Notfallmanagement im Voraus zu planen. Jedoch ist das Notfallmanagement tatsächlich mehr durch die Pandemie in Schwung gekommen. Zuletzt erklärt Herr Naake, dass es oft schwer ist, potenzielle Angriffspunkte, Schwachstellen und „kritische Kronjuwelen" eines Unternehmens vor einem Angriff zu finden.

5. Wie würden Sie IT und Cybersicherheitsrichtlinien in den USA zu Deutschland oder der EU vergleichen?

Herr Naake hat das Gefühl, dass sich viel in den USA bei diesem Thema momentan bewegt. Die USA haben ähnliche Gesetze wie in Deutschland oder der EU, jedoch finden mehr Audits in den USA statt, was zu besserer IT und Cybersicherheit führt. Das Problem in Europa ist, dass viele Unternehmen sich an ISO Standards richten und lediglich ISO als eine Voraussetzung sehen. Hier werden keine offiziellen Audits durchgeführt und somit können Firmen leicht IT-Sicherheitsstandards vortäuschen.

6. Wie schaut der Audit Prozess bei EY aus?

Herr Naake erlärt, dass es beim Audit um ein Scoping der Systeme handelt, wobei kritische Systeme identifiziert werden. Es werden auch viele Screenings, Zugangsproben und Stichproben in verschiedenen Bereichen des Unternehmens gemacht, wie zum Beispiel bei Human Resources. Technisch werden Schwachstellen, Berechtigungen, Zugriffe und Passwort Einstellungen geprüft.

Translated Version:

1. The NIS Directive is considered the first official cybersecurity directive in the EU. Can you explain how this directive was adopted in German critical infrastructure and how it complemented the KRITIS regulation?

Mr Nakke explains that the NIS Directive is the EU's framework for information security. He adds that there is a difference between cyber security and information (IT) security. Cybersecurity is about external attacks, and in IT security, most failures occur during change management. In most cases, the NIS Directive steers IT security. Mr Naake explains that Germany already published its own IT security law in 2015 before the NIS directive was enacted in 2016. He emphasizes here that the NIS Directive is only a framework, as it is a directive. Mr Naake deals with so-called KRITIS sectors (critical sectors), such as hospitals. Different KRITIS sectors have different thresholds that you must register with the German Federal Office for Information Security (BSI). The threshold for hospitals, for example, lies at 30,000. After registering the threshold, the appropriate IT security technology is finally implemented. Mr Naake advises me to look at the Open KRITIS site. In Germany, something unique is the obligation for firms to be audited every two years. In this process, someone

external comes to the company and checks whether the required IT security standards are implemented.

2. What restrictions did you see in the NIS Directive? What are you hoping for in the NIS 2 Directive?

Mr Naake mentions that the NIS 1 Directive was too vague and crude. Local laws differed a lot, for example in IT security obligations, but also in the critical infrastructures involved. Since Germany performs mandatory audits, IT security standards are automatically implemented. This is not the case in most EU member states. Austria has been partially aligning itself with Germany in terms of IT security since 2015, but there have been more requirements in Germany. With the NIS 2 Directive, Mr Naake hopes for more audit obligations, but this will probably not be the case. Something that will improve, however, is the concretization of affected companies in the NIS 2 Directive.

3. Can you tell me more about the KRITIS IT law? What is the difference between the IT Security law and the KRITIS IT law?

Mr Naake explains that the KRITIS IT law has existed since 2017 and assigns thresholds, as well as sectors in the IT security of critical infrastructures. Since 2018, Mr Naake has been conducting reviews and audits with his team based on this law. An additional task for him is to perform transformations at companies that implement the KRITIS law. He additionally explains that the Institute of Public Auditors in Germany (IDW), with the support of the BSI, has created a catalogue of requirements for the concretization of KRITIS. The IT Security law was published in 2015 and is the framework for IT security in Germany. However, both laws are interrelated.

4. In your opinion, what are the biggest challenges in setting up IT security standards at companies and critical infrastructures?

Mr Naake sees challenges particularly in production IT (OT). This is the case because a lot of OT is controlled by machines and some of these still have old operating systems. The danger with OT operating systems is often ransomware, a worm that infiltrates company software. What Mr Naake also sees as a challenge is emergency management in the event of an IT/cyber-attack. Many companies find it difficult to plan emergency management in advance. However, emergency management has received more attention due to the pandemic. Lastly, Mr Naake explains that it is often difficult to find potential attack points, vulnerabilities, and "critical crown jewels" of a company before an attack has taken place.

5. How would you compare IT and cybersecurity policies in the US to Germany or the EU?

Mr Naake feels much is currently happening in the U.S. regarding this topic. The U.S. has similar laws to Germany and the EU, but more audits take place in the U.S., which leads to better IT and cybersecurity. The problem in Europe is that many companies follow ISO standards and only see ISO as a requirement. Here, no official audits are conducted and thus companies can easily fake IT security standards.

6. What does the auditing process look like at EY?

Mr Naake explains that the audit is a scoping of systems, where critical systems are identified. A lot of screening, access sampling, and random sampling takes place in different areas of the

company, such as Human Resources. From a technological point of view, vulnerabilities, authorizations, accesses, and password settings are checked.