E.U.’s impact on a borderless cyberspace

Smits, Kevin

E.U.'s impact on a borderless cyberspace

Kevin Smits
S3124088

Master Thesis, Executive Master Cyber Security

Supervisors
Dr. T. Tropina
Prof.dr. B. van den Berg

19 January 2023

Table of contents

List of acronyms

AI	Artificial Intelligence
CA	Certificate Authority
CSIRT	Computer Security Incident Response Team
DNS	Domain Name Server
eIDAS	Electronic Identities And Trust Services
EPD	ePrivacy Directive
EPR	ePrivacy Regulation
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization of Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
LGPD	General Data Protection Law
NIS	Security of Network and Information Systems
OSI	Open Systems Interconnection
PGP	Pretty Good Privacy
POPIA	Protection of Personal Information Act
QWAC	Qualified Website Authentication Certificates
TCP-IP	Transmission Control Protocol/Internet Protocol
UK	United Kingdom
URL	Unified Resource Locator
US	United States
WWW	World Wide Web

1. Introduction

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather[1]. – John Perry Barlow 1996.

Cyberspace, a digital domain that, according to John Barlow, does not exist in the physical world[2]. This new domain allows users to connect to anyone anywhere at any time, as long as they had a connection with the Internet. As a result, people could digitally cross the physical borders and visit websites or chat with people from another country. Its initial usage was for the U.S. Defense Department and those it had contracts with, but it exploded once it became available to the public thanks to its interoperability of underlying infrastructure as we'll explore later[3]. However, this fast and widespread usage means that users of cyberspace are likely not aware that they are using such a borderless technology and therefore not adhere to local laws and customs[4]. It can be argued that this was the entire idea behind this new technology.

Since its origin discussions have taken place on how, or even if, to govern this new domain called cyberspace. Here we can identify two opposing sides at the early stages of cyberspace. On the side there is the desire for not having any governing as is clearly stated in "A Declaration of the Independence of Cyberspace" [5], where John Perry Barlow asks the governments from the world not to interfere with cyberspace and essentially leave it borderless. The governments themselves were debating on how to govern this space and impose law, and regulations[6], when the users are in different countries and are therefore out of reach for the governments imposing it. Precedents have been set here, e.g., by Yahoo! Case, where a U.S. company had to comply with French law[7].

Today's debate has shifted to digital sovereignty and the inherent danger a borderless medium like the Internet brings. Here it is no longer just about law and regulation, but often rather regarding national security[8]. Over the past years cyberattacks have become more impactful as more and more systems are connected to the Internet. In the 2015 cyberattack on Ukraine entire parts of the country were in a black-out during the cold winter after a state sponsored attack on the power grid[9]. Other threats in cyberspace

[1] Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Davos, Switzerland.

[2] Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Davos, Switzerland.

[3] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.

[4] Nagy, T. B. (1998). Personal Jurisdiction and Cyberspace: Establishing Precedent in a Borderless Era. CommLaw Conspectus 101.

[5] Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Davos, Switzerland.

[6] Kleinwächter, W. (2004). BEYOND ICANN VS ITU? How WSIS Tries to Enter the New Territory of Internet Governance. (66 (3–4): 233–51). London: Gazette: The International Journal For Communication Studies. doi:10.1177/0016549204043609

[7] Reimann, M. (2003). Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage. (24.3). Michigan Journal of International Law. Retrieved from https://repository.law.umich.edu/mjil/vol24/iss3/1

[8] Claessen, E. (2020). Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. (5.1). Journal of Cyber Policy. doi:I: 10.1080/23738871.2020.1728356

[9] Kostyuk, N., & Zhukov, Y. M. (2019, 02 01). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? (63.2), 317-347. Journal of Conflict Resolution. doi:10.1177/0022002717737138. ISSN 0022-0027. S2CID 44364372

have taken place as well, e.g., with the use of disinformation with the Cambridge Analytica scandal[10]. This leads to the securitization of the internet infrastructure[11]. Securitization means that 'an issue is given sufficient saliency to win the assent of the audience, which enables those who are authorized to handle the issue to use whatever means they deem most appropriate. As a result, state actors are increasing their focus on achieving an Internet that is secure and resilient'[12]. These changes in cyberspace and volatility at an international stage brings the two sides identified at the early stages of cyberspace closer together. It is the reason why cyberattacks are facilitating the debate on cybersecurity. As Milton Mueller[13] states these new challenges, under the flag of cybersecurity, are "used to enmesh various aspects of the Internet in foreign policy and military conflicts, as well as in other national forms of regulation and control in which states are privileged". The public is more open to forms of governing of cyberspace ergo state actors are attempting to govern cyberspace, or the Internet. Nations do so through different forms of authority on cyberspace. These forms can be grouped into two sides, also known as spheres of authority. Daniëlle Flonk, et al, describes these as the liberal sphere and the sovereign sphere[14].

Both spheres are identifying cyberspace as a domain for military action and this characterization led to efforts to provide normative frameworks for cyber protection. This possible militarization of the Internet provides new options for the challenges state actors face when trying to provide security for their citizens. Maria Ristolainen describes it as "both Western and Russian cyberspace and/or information space is becoming a new space within which states may act and reassert traditional notions of sovereignty – yet through contradictory "open" and "closed" approaches'[15]. The West and Russia with their respective "open" and "closed" approach can be compared to the liberal and sovereign sphere. Using these two as example, shows how different their approaches are towards governing the Internet.

The sovereign sphere with its closed approach perceived the Internet as a threat to their sovereignty and therefore should be under a high level of control by the government. Countries like Russia, China and Iran epitomize the idea of sovereign power over internet within state borders[16]. For example, Russia's closed approach focuses inwards on how to achieve control for themselves[17]. Their 'autonomous Russian Internet' demonstrates a state's attempt to secure and centralize control over its cyberspace. It consists of a set of laws that essentially allows Russia to set rules for using cyberspace and introduce a digital border that they can enforce through regulation of the routing of traffic. It allows the limitation of access to resources the

[10] Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. Information Polity, pp. 429-434. doi:10.3233/IP-180009

[11] Buzan, B. G., Waever, O., & de Wilde, J. H. (1998). Security: A New Framework for Analysis. Lynne Rienner, p. 247.

[12] Balzacq, T., Léonard, S., & Ruzicka, J. (2016). Securitization' Revisited: Theory and Cases. International Relations, pp. 494-531.

[13] Meuller, M. (2017). Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings. Digital Policy, pp. 415-428.

[14] Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020, 07 01). Authority conflicts in internet governance: Liberals vs. sovereigntists? Cambridge University Press, pp. 364 - 386. doi:10.1017/S2045381720000167

[15] Ristolainen, M. (2017). Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security within Russia and the West. Journal of Information Warfare, pp. 113–131.

[16] Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020, 07 01). Authority conflicts in internet governance: Liberals vs. sovereigntists? Cambridge University Press, pp. 364 - 386. doi:10.1017/S2045381720000167

[17] Ristolainen, M. (2017). Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security within Russia and the West. Journal of Information Warfare, pp. 113–131.

government deems not allowed, to the extent of completely preventing traffic[18]. Digital traffic in Russia is only going through approved internet exchange points that are required to adhere to Russian regulations[19]. In addition, Russia is exploring their options for implementing a duplicate infrastructure to ensure the security and operability of internet in Russia[20]. It can be imagined that content and traffic being blocked in such a manner impacts a cyberspace and its inherently borderless nature heavily.

Contrary to the sovereign sphere, the liberal sphere with their open approach, perceives the Internet as an opportunity and wants it to be governed by private self-regulation with a minimal role for the state. The internet infrastructure and architecture does not support a top-down regulation according to the idea of self-regulation. As Milton Mueller describes this way of freedom of the Internet as 'engineered into its protocols'[21] The state does provide a certain level of security and can enforce law and regulation when needed. Beyond that, the governance of the Internet is based on a multi-stakeholder model and thus providing as much freedom as possible. This perspective is predominantly supported by the Western states[22].

In today's debates the term 'digital sovereignty' is still being defined or refined, depending on your perspective. According to Daniel Philpott[23] sovereign authority is exercised within borders, where outsiders may not interfere with its governance. Hobbes and Bodin used even stronger words by viewing sovereignty as absolute and unconditional extending to all matters within the territory[24]. Both descriptions are based on borders surrounding nations, but there are adaptations to how these authorities are implemented. The E.U. is an institution where states give up part of their sovereignty and allow the E.U. to make decisions on these parts. These states still have sovereignty up to a certain degree, but rules and regulations can be pushed from the E.U. to its states[25]. In a way creating a border surrounding all these states, creating an E.U. territory.

These different views on authority in cyberspace and to what extent states want to be sovereign is creating different interventions with the internet's underlying infrastructure. The fact that Russia is trying to implement complete sovereignty, just like China has with their 'Great Firewall', is highly impactful on the workings of cyberspace. These countries are using the traditional borders to start exerting their governance structure. Whereas we see the EU is trying to maintain openness while providing a form of sovereignty as

[18] Government of the Russian Federation. (2019). On the Approval of the Regulations on Conducting Exercises to Ensure the Sustainable, Safe and Comprehensive Functioning of the Internet and the Public Communications Network in the Russian Federation. Gosudarstvennaya Sistema Pravovoj Informatsii.

[19] Government of the Russian Federation. (2019). On the Approval of the Regulations on Conducting Exercises to Ensure the Sustainable, Safe and Comprehensive Functioning of the Internet and the Public Communications Network in the Russian Federation. Gosudarstvennaya Sistema Pravovoj Informatsii.

[20] Ristolainen, M. (2017). Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security within Russia and the West. Journal of Information Warfare, pp. 113–131.

[21] Meuller, M. (2010). Networks and States. MIT Press, pp. 113-131.

[22] Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020, 07 01). Authority conflicts in internet governance: Liberals vs. sovereigntists? Cambridge University Press, pp. 364 - 386. doi:10.1017/S2045381720000167

[23] Philosophy, S. E. (2020, 6 22). Sovereignty.

[24] Lloyd, H. A. (1991). Sovereignty: Bodin, Hobbes, Rousseau. Revue Internationale de Philosophie(45.179), pp. 353-379.

[25] European Commission. (n.d.). Territorial status of EU countries and certain territories. Retrieved from https://taxation-customs.ec.europa.eu/territorial-status-eu-countries-and-certain-territories_en

well[26]. Maintaining a high level of freedom in cyberspace while ensuring sovereignty seems to be difficult without making changes to the inner workings of cyberspace, thus impacting the borderless nature of it. Introducing boundaries or borders in the most common way and according to Forrest Hare "*borders define boundaries for sovereignty regardless of the domain*" [27], thus including cyberspace. It is important to note here that today its under the banner of 'digital sovereignty', but that the reason for control of cyberspace changed over the years. For example, in the beginning of cyberspace it was focused on law and regulation. For this reason we will not focus on the concept of digital sovereignty in this thesis. Recently there has been debate on E.U. impacting the technical infrastructure of the Internet, potentially introducing fragmentation and bypassing the multi-stakeholder governance of the Internet. In this thesis we are looking at cyberspace and the E.U. with their open approach. To what extent is the E.U. able to keep this open approach or are forms of borders or boundaries introduced for its citizens? Or are various E.U. interventions going to impact the global infrastructure of cyberspace and affecting all of cyberspace?

[26] Verstaeger, M. (2019). Answers to the European Parliament: Questionnaire to the Commissioner-Designate: Margrethe Vestager, Executive Vice-President-Designate for a Europe Fit for the Digital Age. Retrieved from European Parliament: https://www.europarl.europa.eu/news/en/hearings2019/commission-hearings-2019/20190910STO60707/margrethe-vestager-denmark

[27] Hare, F. (2006). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? School of Public Policy, George Mason University.

2. Research

A lot is happening on the international stage with cyberspace. An exploding number of new applications being deployed, meeting people around the world through cyberspace, the ability for global shopping and more. Unfortunately, there are also developments that impact the world negatively like cyberattacks, cyberwarfare and exclusion from global cyberspace.

The sphere of authority has profound impact on the workings of cyberspace and therefore its users. The E.U. as part of the liberal sphere has the desire to maintain an open and free cyberspace, while ensuring that its secure and resilient. The impact on the borderless nature of cyberspace from the sovereign sphere can be considered more obvious and raises the question of the impact of the liberal sphere. But will the interventions of the E.U. mean that its users might no longer be able to visit any website on the internet, or will they actively block outside connections? These are the consequences we see at the sovereign sphere of authority. In this thesis we will have a more in-depth look into E.U. interventions that impact the borderless nature of cyberspace. This leads to the following research question:

How do E.U. interventions in the various technical layers of cyberspace affect the (alleged) borderless nature of cyberspace?

This research question is divided into the following sub-questions:

1. *What is cyberspace and its technical layer?*
2. *How do borders apply to cyberspace?*
3. *What are the EU interventions on the technical layer of cyberspace?*
4. *What is the impact of the EU interventions on cyberspace and its borderless nature?*

2.1. Goal

In this thesis we aim to define cyberspace and identify why it is considered inherently borderless. We will focus on the technical layer of cyberspace and analyze the impact of E.U. policy and regulatory interventions on the borderless nature. This will provide insight into the impact on the technical layer of cyberspace by the E.U. in a more holistic way. It can assist policymakers to focus on the desired effect of their interventions and insure the values E.U. has for cyberspace are maintained. These values are an open, free and interoperable cyberspace[28].

2.2. Approach

The theoretical framework will establish the basis to work from by defining cyberspace and its technical layer. We will explore why it can be considered borderless through its technical architecture. Here we will look at the physical infrastructure, standards and the protocols used by the Internet. Next, we will have a closer look at borders in general and how these apply to cyberspace.

[28] Tiirmaa-Klaar, H. (2016, June 20). EU International Cyber Policy: promoting a free and secure global cybespace. Retrieved from Global Forum on Cyber Expertise.

Next, in chapter 4, we will explain the scope of this thesis, introduce the framework for analysis and provide critical reflection on the approach.

In the analysis chapter, we will examine the interventions and analyze them with based on the conceptual model of cyberspace. This allows us to identify which interventions impact the technical layer of cyberspace as defined in the theoretical framework. By further analyzing the interventions we will assess how they impact cyberspace and its borderless nature. The thesis will end with conclusions and further research recommendations.

3. Theoretical Framework

The first step in our analysis is to provide a common understanding of what is cyberspace. To define cyberspace, we will look at various definitions from different perspectives and explore its technical architecture. Next, we will explore the concept of borders and how they apply to cyberspace.

3.1. Cyberspace

3.1.1. Definition

There is no single definition that describes cyberspace at the scientific level[29], in fact every government, academic institute and in some cases even organizations use their own definitions. To understand cyberspace, we will look at a few different definitions from these sources to identify the elements that make up cyberspace. For this first view of a definition of cyberspace we will use a few often quoted definitions.

Definitions of cyberspace by governments and international organizations.

Ministry of Defense U.K., Deputy Secretary of Defense Gordon England, 2008: *"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."* [30]

Federal Ministry of the Interior Germany, Cyber Security Strategy for Germany, 2011: "*The virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.*"[31].

Department of Defense, Dictionary of Military and Associated Terms, 12 April 2001 (*amended 2007*): *"The national environment in which digitized information is communicated over computer networks"*[32].

Department of Defense, Dictionary of Military and Associated Terms, 12 April 2001 (*amended 2009*): *"A global domain within the information environment consisting of interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers."*[33].

International Telecommunication Union (ITU), ITU National Cybersecurity Strategy Guide (2011): *"systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks."*[34]*.*

[29] Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009, April 1). Cyberpower and National Security. National Defense University Press.

[30] Ministry of Defense UK. (2008). Deputy Secretary of Defense Gordon England.

[31] Federal Ministry of Interior Germany. (2011). Cyber Security Strategy for Germany.

[32] U.S. Department of Defense. (2001). Dictionary of Military and Associated Terms (amended 2007).

[33] U.S. Department of Defense. (2001). Dictionary of Military and Associated Terms (amended 2009).

[34] Wamala, F. (2011, September). ITU National Cybersecurity Strategy Guide. International Telecommunication Union.

> The International Organization for Standardization (ISO), Guidelines for cybersecurity, 2012: *"the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"*[35].

These definitions can significantly differ from each other and might not cover the same scope. To provide a more single and complete definitions Daniel Kuehl researched the different definitions to combine the best elements[36]. As a result, the best elements from different definitions are used to develop one that covers the other definitions too. The interconnected and interdependent networks of information and systems are present in both the physical and digital world, within and outside of traditional geographic boundaries. It shows the use of information and communication through an underlying technical infrastructure.

"Cyberspace is a global domain within the information environment whose distinctive and unique character is frames by the use of electronic and electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies." [37]

3.1.2. Conceptualizing Cyberspace: Three Layer Model

Looking at cyberspace as a concept is another available approach. A three-layer model was developed to conceptualize cyberspace by identifying three distinct layers and the different sectors active in cyberspace[38]. These layers expand from the technical layer required to operate cyberspace and includes the technology with its infrastructure. The socio-technical layer that envelopes the previous layer and encompasses the social interactions taking place. Lastly is the governance layer that consist of rules and regulations required to control the other layers.

Technical Layer

This conceptualization of cyberspace identifies three layers that are present in all cyber sub-domains, or often named sectors and industries. The middle of the model, and basis of cyberspace, is the technical layer. It focuses on the building blocks to technically enable cyberspace with at its core the physical infrastructure with ethernet cables, satellites and information systems and expanding with their communication methods based on the famous TCP-IP protocol stack.

Socio-Technical Layer

The layers expand from the technical building blocks to enable the enormous variety of cyber activities people use today. It focuses on the interactions between the users of cyberspace and cyberspace itself.

[35] The International Organization for Standardization, & The International Electrotechnical Commission. (2012). ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity.
U.S. Department of Def

[36] Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. National Defense University Press.

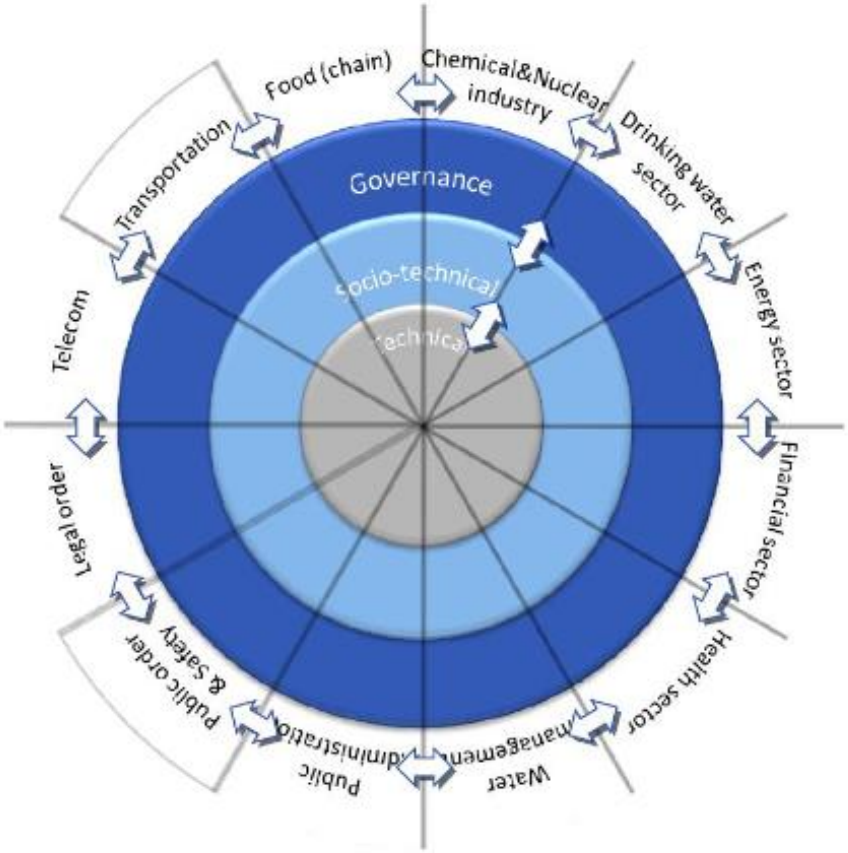
[37] Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. National Defense University Press.

[38] Berg, J. v., Zoggel, J. v., Snels, M., Leeuwen, M. v., Boeke, S., Koppen, L. v., . . . Bos, T. d. (2015). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. NATO Science and Technology Organization.

With its current 5 billion users[39] it is a complex environment that enabled activities from simple information retrieving and sharing to cybercrime to creating and maintaining complex ICS systems.

Governance Layer

On the outside is the governance layer that indicates the governance on both the socio-technical and the technical layer of cyberspace. It focuses on the methods, e.g., standards, regulations and law, used for influencing the other layers by human actors, organizations or even entire nations.



3.1.3. Internet or Cyberspace

Some of the definitions included “the Internet” and many people will assume these are the same. It is because the internet is often considered as a synonym for cyberspace, this is not the case as there is more to cyberspace than just the internet. The Internet is the infrastructure on which cyberspace is build and a good place to start exploring why it was considered borderless.

The origins of the Internet started decades ago, when government researchers started using a new way of sharing information in the 1960s and is considered a predecessor of the Internet. The large and immobile computers were not digitally connected as today, so to share information one needed to physically travel

[39] Number of internet and social media users worldwide as of July 2022. (2022). Retrieved September 2022, from Statista: https://www.statista.com/statistics/617136/digital-population-worldwide/

to retrieve the information, or it had to be shared through post. Towards the end of the 1960s, during the cold war, the United States Defense Department envisioned a way to share information even if a nuclear war broke out. The result of this vision was ARPANET (Advanced Research Projects Agency Network). A network that allowed different computers to communicate with each other over great distances. Though a great success, its membership was limited to the Defense Department and those who it had contracts with. As a result, other networks sprouted into existence to provide the same functionality in information sharing. In 1982 ARPANET deployed TCP/IP to their network and in 1983 all traffic had to use TCP/IP to operate on, from that moment on, the Internet. All communications between networks and systems are done through a universal language. This ultimately led to the widespread use of the internet as we know today[40].

The Internet can be considered as the basis of cyberspace, and this is where the two differ. Cyberspace requires the Internet to operate as it contains the technical architecture and build on top of that by facilitating social interactions that happen through the Internet.

3.1.4. Technical Architecture

Understanding the technical architecture is best done using a layered model approach and shows where cyberspace continuous and the Internet ends. Such a model was developed to explain the function of components of the Internet based on these layers and how they cooperate to transfer "Internet traffic". It is a conceptual tool that presents a breakdown of the components from the technical layer of the "conceptualizing cyberspace: three-layer model" into hierarchical stacks. Different stacks of layers have been developed as a layered model, ranging from a simplified and distinct two stack[41], to a more complex and well known OSI-model seven layered stack[42]. The differences between the models are based on the analysis of the conceptual tool and not significant as the same information is present in all models. It is just simply grouped versus separated. To avoid unneeded complexity and oversimplification we will use the four layered stack from Werbach[43] to guide us through this technical architecture. Physical Layer

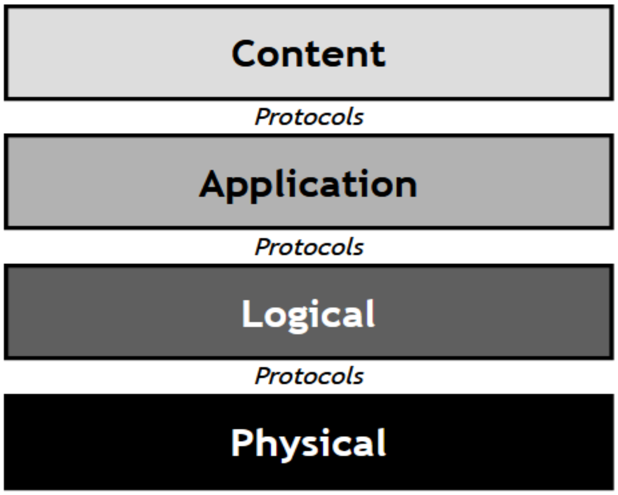


Figure 2: Werbach's Layered Model for Internet Policy

The base of the conceptual stack is the hardware required to operate the Internet, the physical layer. In its essence this is the physical connection required to operate and functions as a medium to transmit information. This physical aspect is the hardware that consists of servers, routers, satellites, cables, and other communication technologies, essentially every piece of physical equipment required to operate the

[40] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.

[41] Moose, J. (2012). Two Stack Layered Model. pp. 80-83.

[42] ISO. (1994). ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model.

[43] *Werbach, K. (2002). A Layered Model for Internet Policy. J. on Telecomm. & High Tech. L 37.*

Internet. An important part of this are the Internet backbones and telecommunications networks as they provide this physical infrastructure that allows data to flow in between[44].

Internet backbones are formed by a group of service providers that connect to autonomous networks to route information transfers between them. Access to this connection is sold to providers that connect the end users, both organizations and individuals. These in-between providers are known as the Internet Service Providers (ISP). Internet backbones create their own network that allows all of their users to communicate with each other. Users want to be able to communicate with more than just the users in their backbone and therefore backbones are interconnected with each other. The function of a backbone is only the transfer of traffic and they do not store traffic[45].

When looking at the available connection methods for end users there are many different ones available. For instance, it is possible to connect to the Internet through methods invented for different technologies, e.g., coaxial cable or telephone lines. Nowadays it is possible to use dedicated Internet connections, e.g., fiber-optic cables, Wi-Fi and cellular networks. This diversity in technologies for connecting to the Internet means it has a high level of interoperability. It also means there is a high level of interoperability between the many entities that own these different networks.

Logical Layer

Interoperability of all these different technologies happens on the logical layer. It is where the information is reconfigured to be sent over the physical layer and consists of the protocols that facilitate the transfer of data through the Internet. The physical infrastructure from the previous layer traditionally transferred all data electronically through analog signals but are limited by the technologies that transferred these analog signals[46]. Digitalization through computers changed these limitations by allowing the data to be encoded as standardized data, making it understandable by any receiver and therefore making all communication technologies interchangeable. Effectively allowing every part of the infrastructure to offer the same service, as the same standards are used to communicate.

This is what the Transfer Control Protocol/Internet Protocol (TCP/IP) does and why it is the heart of the Internet[47]. It provides a standardized protocol for transferring data through the Internet. TCP makes it possible to split and reassemble digital information, unlike its analog predecessor. Computers split information into small packages according to the TCP protocol before transferring it over the Internet and label each package, so the receiver knows the order in which to reassemble them. This is what allows the Internet to use any technology for its connections. Next the Internet Protocol adds an unique address to the package so the nodes on the Internet know where to send it. This is called packet switching[48].

Everything connected to the Internet receives this unique address, their IP address, which is an numeric identifier similar to a phone number. An IP address in combination with packet switching allows information to be transferred through a combination of routes to the receiver. This differs from the analog signal that required a continuous direct connection from sender to receiver, also known as circuit switching. As a result,

[44] Werbach, K. (2005). Breaking the Ice: Rethinking Telecommunications Law for the Digital Age. J. ON T ELECOMM . & HIGH T ECH. L. 59 .

[45] Osgood, R. (2004). Net Neutrality and FCC Hack.

[46] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.

[47] *Lessig, L. (2006). Code 2.0: And Other Laws of Cyberspace. BASIC BOOKS.*

[48] Brate, A. (2002). Techno Manifestos.

the Internet did not require centralized operators to facilitate the connections, but rather relied on decentralized nodes that packages transfer through. This means more efficient transfer speeds and allows for load distribution on the network[49]. It means that sending information through the Internet means it is broken down into packages, these packages are labeled and sent to the IP address. These packages can follow the most efficient available path through different geographically located servers to the receiver and do not need to arrive in order as they are labeled in orders so the receiving system can order them after receiving them.

TCP/IP allows the transfer of information, regardless of what this information is. The Internet also does not register what this information is, it just transfers it to the next node until it reaches the intended receiver. It is the reason why the Internet can be called “stupid”. Its design allows information to move freely over the Internet[50]. An important note is that the Internet is not a single network, but rather a collection of networks that use the same protocols to operate and therefore ensure interoperability.

It is important to understand that the logical layer can be considered the heart of the Internet as it is the link between the physical infrastructure from the layer below and the application layer above. It is the core of the Internet’s interoperability through its use of an open network architecture, that is the technical purpose of the Internet[51]. An open network architecture is the use of a common media independent protocol and open interfaces to transfer information[52].

The Application Layer

The logical layer is all about sending packages across the Internet and providing this functionality regardless of content, sender or receiver. It is where the previous statement of the Internet is stupid comes from, as it is an end-to-end network where the "smart" part happens on the endpoints. The Internet was designed to run as a general infrastructure that allows different, and therefore new, applications to use the already existing infrastructure. The application layers sit at the end of these networks and consist of these applications that use the Internet[53].

The most common way to use the Internet is the World Wide Web (WWW) and an ideal example to guide us through this layer[54]. The WWW is an application on the application layer and is executed on the endpoint, or the device of the user[55]. We will use this application to explain the workings of the application layers and the end-to-end principle. In the logical layer we've seen the IP address as a numerical unique number to identify the device on the Internet. People are usually not able to remember these numbers easily, so the WWW is designed to use a Uniform Resource Locator (URL), e.g. https://www.universiteitleiden.nl/, to allow its users to visit websites more easily. Users can just simply type the URL in the web browsers address

[49] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.
[50] DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.
[51] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.
[52] Open Network Architecture (ONA). (n.d.). Retrieved from Dialogic: https://www.dialogic.com/glossary/open-network-architecture-ona
[53] Lessig, L. (2006). Code 2.0: And Other Laws of Cyberspace. BASIC BOOKS.
[54] Betz, D. J., & Stevens, T. (2011, November 30). Cyberspace and the State: Chapter One: Power and cyberspace. pp. 35-54. doi:10.1080/19445571.2011.636954
[55] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.

bar. The browser application sends a request to a server that contains a list with all addresses that end with, in this example, .nl via your ISP[56]. It identifies the URL from the list, also known as the root file, and translates it to the IP address of the device that hosts the URL through the Domain Name System (DNS). Simply put, it translates https://www.universiteitleiden.nl/ to 132.229.29.70. The server then is connecting to its directory named "www" to and the browser will look for the "index.html", which is often the default file. A copy is transferred to the device that requested the connection and is stored on the device itself. The index file is locally opened on the device and this file contains the code that tells the browser what to display for its user. The entire process is transferred by the physical layer and is made possible by the logical layer.

Information accessed this way is stored on the server and device requesting the information. It demonstrates that information is not stored on the Internet but made accessible through the Internet[57]. The use of the information happens on the device and can be manipulated by the software available on that device. Essentially this is the end-to-end principle of the Internet through the common protocol. This architecture allows the diversity of applications to run on the same underlying network, the Internet. As a result, the number of applications and networks have exploded since its creation[58].

One of these is the Internet of Things (IoT) that allows devices other than computers to connect to the networks and run applications. IoT makes it possible for any almost device to be connected to the Internet, nowadays there are light bulbs that are connected. Innovations happen at the applications layer because the logical layer protocols are open source, meaning anyone can develop an application using the Internet. This means that anyone can change how the Internet communication works, for example the Pretty Good Privacy (PGP) program. PGP is a public key encryption program that allows for encrypted messages to be sent over the Internet[59].

The Content Layer

Users are usually only interested in the content when using an application and do not care about the code of the application nor the rest of the underlying technical architecture. In the cyberspace there are different kinds of content, most common are words, images, videos and sounds. But, the Internet is able to transfer anything that can be digitalized. An interesting example is Thingiverse, an online repository of 3D objects that can be directly printed by 3D printers at home[60]. The 3D blueprint available at Thingiverse is transferred from the server to the user through the other layers and, after printing, the users have a physical object received through the Internet. This demonstrates that anything can be developed at the application layer if there is connectivity on the logical layer, and it can be digitalized. The content layer is the output of the end devices.

How to regulate the Internet is a question that is usually asked regarding this layer[61]. It happens on this layer because the stacking of the layers below allow data, especially large amounts, to be transferred to anyone anywhere with network access in an instant. The content layer existed before in other media. For

[56] DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.

[57] Tambini, D., Leonardi, D., & Marsden, C. T. (2008). Codifying cyberspace : communications self-regulation in the age of internet convergence.

[58] *Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.*

[59] Greenberg, A. (2012). This Machine Kills Secrets. Dutton.

[60] https://www.thingiverse.com/

[61] Bailey, J. (2004). Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation. Manitoba Law Journal Vol 30 No 2.

example, the television is a broadcast medium that allows a centralized sender to reach many users at once. This was one directional and therefore easier to control through regulation when desired. Another example is the telephone that provided bidirectional interactions, but only on a small scale. Therefore it was acceptable to not have regulation as it did not have the same reach as the Internet. The Internet is both bidirectional and capable of reaching many users. As a result, there is low control over the information spreading over the Internet and the information reaches far with its possible implications[62].

Debate on regulation and thereby governance of the Internet is mostly about censorship versus free speech on the content layer.[63] This is because the layers underneath is primarily about the flow of information. This information flows across networks that are decentralized, therefor capable of ignoring traditional borders.

3.1.5. Conclusion

Cyberspace is a subject that does not yet have a single definition or description available. What we can conclude is that is consists of the Internet with its technical architecture, information and social interactions. Its technical architecture consists of physical infrastructure, protocols and applications, that allows cyberspace to exist. For this thesis we will use the definition provided by Daniel Kuehl. The Internet can be considered global thanks to the interoperability provided by the common language that consists of the standardized protocols and unique identifiers. It is what holds the other layers together and enables the global connectivity we know and use today. The technical layer of the conceptualization of cyberspace is further defined by the technical architecture of the Internet, ergo the four layered stack from Werbach.

3.2. Borders and Cyberspace

Cyberspace is the new domain in which people reside, though it is only in a digital form without the physical presence people are used to. This makes borders in this domain a new concept as where traditionally borders started on land, expanded to sea when ships came and air when planes were invented, the next domain to figure out how borders apply is cyberspace. When the concept of cyberspace started it was not governed by any government and its users were keen on keeping it that way. In 1996 John Perry Barlow wrote "A Declaration of the Independence of Cyberspace"[64] in which he specifically asks governments to not interfere with cyberspace in any way. According to John Perry Barlow this new domain should be self-governed with their own legal institute to solve online disputes. This comes from the idea that as all legal concepts used by governments apply to things based of 'matter', whereas there is no matter in cyberspace[65]. The claim that cyberspace does not exist in the physical world has been challenged on the fact that it requires a physical infrastructure to operate and users, that are both geographically located somewhere around the globe[66]. Interestingly Barlow still stood behind his declaration in 2016[67].

[62] *EUTELSAT. (2012). Eutelsat Condemns Jamming of Broadcasts From Iran and Renews Appeals for Decisive Action to International Regulators. Paris.*

[63] Ibarrondo, M. R. (2012). The Censorship-Free Speech Dichotomy in the Internet: an overview.

[64] J. P. Barlow, "A Declaration of the Independence of Cyberspace," Davos, Switzerland, 1996.

[65] J. P. Barlow, "A Declaration of the Independence of Cyberspace," Davos, Switzerland, 1996.

[66] Graham, M. (2013, 3 1). Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? The Geographical Journal. doi:10.1111/geoj.12009

[67] Greenberg, A. (2016, 8 2). It's Been 20 Years Since This Man Declared Cyberspace Independence. Retrieved from https://web.archive.org/web/20160211000415/https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/

3.2.1. Traditional Borders

The concept of borders has been present and important throughout history. A border is the demarcation, by a real or artificial line that separates areas based on geographical basis. This separation results in countries, provinces, cities and more. The difference between these areas is the governing body that controls the outlined area by borders. This governing body provides protection for its citizens and can only create and enforce laws within its borders[68].

Historically these borders could change over time through violent take-overs, trading and selling or being divided after war through international agreements. These borders can follow natural boundaries like mountain ranges or bodies of water. Within borders people can usually travel, work and reside freely, but crossing borders for any of those activities can be constricted by local law and regulation[69]. The United States is a good example that limits non-citizens on their ability to work or travel within its borders. They issue permanent resident cards, also known as green cards, that allow non-citizens to work and live within their country and be under the protection of their law[70].

3.2.2. Applied to Cyberspace

Working from the idea that governments want to protect the people within their borders and enforce their laws, it has become essential to identify how laws can be applied to cyberspace. In the physical world it is obvious when a foreign threat becomes a domestic threat as it is required to cross the borders which are well established. Once within the borders threats, both foreign and domestic, can be addressed by local law. It becomes less obvious when we look at cyberspace, when criminals or terrorist want to attack, they can do so from their own country with its own laws. Especially since it is possible to attack critical infrastructures from these distances without people having to cross a physical border. This means the definition of border security has changed radically.

In contrast to defining the physical border and defending it from foreign cyber threats, the government's role in cyberspace has traditionally been more focused on handling a cyber incident after it occurred and lets the defending up to private entities[71]. To use a metaphor for this approach, and show the potential consequences of this role, would be letting people living at the border be responsible for the physical border security. A thought shared by many is that cyberspace has no borders and is a more open world and society, it is not as simple as that. The physical infrastructure travels through nations and therefore borders. This means the data is present in the nation that it originates from and the nation in which the user accessing the data resides.

Examples of how the physical borders apply to cyberspace are available. One of these examples is China's Great Firewall, that blocks large sections of cyberspace for users within China[72]. It is using a traditional border to ensure the government has complete control over its cyberspace. Another example is the General

[68] Raffestin, C. (2012). Space, territory, and territoriality (30 ed.). Environment and Planning D: Society and Space. doi:10.1068/d21311

[69] Raffestin, C. (2012). Space, territory, and territoriality (30 ed.). Environment and Planning D: Society and Space. doi:10.1068/d21311

[70] Border. (n.d.). Retrieved from National Geographic: https://education.nationalgeographic.org/resource/border

[71] Hare, F. (2006). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? School of Public Policy, George Mason University.

[72] Lee, J.-A., & Liu, C.-Y. (2012). Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. Minn. J.L. Sci. & Tech.

Data Protection Regulation (GDPR)[73]. The GDPR is E.U. regulation on privacy and data protection that provides citizens control over their personal data. This control is both national (states within the E.U.) and international (outside of the E.U.). Though this regulation is developed for E.U. citizens only, meaning the application of a traditional border, it ended up having a larger cross-border impact. Companies like Microsoft implemented GDPR for all its users globally[74], whereas Facebook deployed parts of the GDPR for all of its users[75]. This effect is also known as the Brussels Effect[76]. Simply put, regulation is developed unilaterally and ends up being used globally. This example is on the socio-technical and governance level of cyberspace.

3.2.3. Fragmentation

It is argued that when borders are applied to cyberspace on a technical level, fragmentation is introduced as the Internet no longer 'just works' for its users[77]. Internet fragmentation, also known as balkanization or splinternet, is the breaking up of the Internet into different segments that are no longer connected as we know today. This has been a growing concern with the increased focus on digital sovereignty[78]. There is no agreed definition on fragmentation available yet. Milton Mueller describes our current Internet as 'unifraged', as the Internet is unified and fragmented at the same time[79]. This is because the Internet is not a single network, but rather a collection of networks that use the same protocols to operate and therefore ensure interoperability. It is the loss of connectivity that introduces fragmentation and splits the Internet into smaller networks. Changes in the technical architecture can introduce fragmentation on the technical layer, because it can alter the common language or infrastructure used that enables its interoperability[80]. As a result, users cannot access sections of the Internet because their devices can't 'talk' to the other devices on the Internet. As Tatiana Tropina describes it: *"At its technical layer, the Internet would only 'fragment' if it lost its interoperability: for example, if connected devices or autonomous systems were to use incompatible protocols or if other unique identifier arrangements were to compete with the currently prevailing system. As long as the Internet uses the same universally accepted standards, it does not splinter in its technical layer"*[81]. Fragmentation again highlights that the technical layer, which is going to be the focus of this thesis, is the core of the Internet's global connectivity.

3.2.4. Conclusion

There is a clear definition of borders and examples of how they apply to different aspects of the physical world. However, cyberspace is a more complex environment in which traditional borders are not so easily

[73] When Regulatory Power and Industrial Ambitions Collide: The "Brussels Effect," Lead Markets, and the GDPR. (2022). Privacy Symposium, pp. 129-151.

[74] Brill, J. (2018, May 21). Microsoft's commitment to GDPR, privacy and putting customers in control of their own data. Retrieved from Microsoft: https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/

[75] Egan, E., & Beringer, A. (2018, April 17). Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live. Retrieved from Meta: https://about.fb.com/news/2018/04/new-privacy-protections/

[76] Bradford, A. (2012). The Brussels Effect. Columbia Law School.

[77] Plexida, E. (2022). EU Dimensions of the 'Splinternet' Question. *Centre for Global Cooperation Research*.

[78] Tropina, T. (2022). Internet Fragmentation: What's at Stake? *Centre for Global Cooperation Research*.

[79] Meuller, M. (2017). Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. Cambridge: Polity.

[80] Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). Internet Fragmentation: An Overview. Davos: World Economic Forum.

[81] Tropina, T. (2022). Internet Fragmentation: What's at Stake? Centre for Global Cooperation Research.

implemented. This is especially true when we are talking about the technical layer of cyberspace. It is borderless because the Internet operates as one giant network through global connectivity, combining different smaller networks by using the same standards and protocols. Changes in these standards and protocols that are not adopted globally will result in fragmentation and lead to borders that do not allow the Internet to 'just work' for its users. In essence the entire technical architecture, from the interoperability of the physical infrastructure to the common communication protocols with the following structures allows cyberspace to have its global connectivity and be considered borderless today. Another way the Internet would not continue to just work for its users would be blocking traffic transferring across the Internet within the technical architecture. An example would be placing a firewall, like China, that would introduce this 'feature' and introduce a traditional border in cyberspace.

4. Methodology

This thesis will examine the phenomenon on impact of policies on the borderless nature of the Internet through a case study of the E.U. The E.U. was selected because it is part of the liberal authority sphere where the values for cyberspace are to have it open, free and interoperable[82]. Though wat makes it an interesting case study are the various concerns that some regulation might impact these values[83] [84]. Currently the EU is seeking to intervene on the technical layer through law and regulation, because it is concerned over its digital sovereignty. In addition, the availability of information is better compared to other countries that intervene with the technical layer, like China and Russia. Also, the E.U. has proven to initiate exemplary legislation that end up being used globally in one form or another, like the GDPR[85]. Part of this chapter is to explain the scope, describe what interventions are, set a framework for borders and identify which are analyzed in this thesis. It is also important to discuss the limitations of the analysis.

4.1. Scope and limitations

The scope for analysis in this thesis consists of three parts. Firstly the European Union's policies and regulations related to cyberspace selected as described in chapter 4. The second part of the scope is the technical layer of cyberspace. This layer is the reason cyberspace thrives as a borderless medium and can have the biggest impact on its borderless nature through interventions. These interventions can have a negative impact, but also positive. Lastly there are specific interventions selected. Here we focus on the more recent policies and regulation. This distinction is made because of the increased attention cyberspace and cybersecurity/digital sovereignty has received since the increase in cyberattacks in recent years. With this in mind the available policies and regulations on cyberspace are reviewed and can be found in chapter 4.2.This thesis has limitations regarding the extent to which policies or regulations can or will be implemented in the future, but rather focuses on the information as provided by the E.U. official policies and regulations pertaining to interventions. To a degree this means that it expects the policies and regulations to be implemented to its fullest, comments on the feasibility of it will be made but not explored.

4.2. Framework

Describing a framework to analyze the interventions within the policy and regulation documents from the E.U. requires a description of what is understood with an intervention. For this concept of 'interventions', it is often the case that debates revolves around what is preceding the word intervention, e.g., 'humanitarian' or 'legitimate'. However, the actual word intervention is taken for granted. Christian Reus-Smit argues that interventions can comprise of multiple units of authority, with their own jurisdiction. Interventions are not required to be territorial but can also be functional for example. As Christian Reus-Smit describes *"International intervention is the transgression of a unit's realm of jurisdiction, conducted by other units in an order, singly or collectively. Interventions are always transformative; they are transgressions to reconfigure identities, institutions, and practices"[86].*

[82] Tiirmaa-Klaar, H. (2016, June 20). EU International Cyber Policy: promoting a free and secure global cybespace. Retrieved from Global Forum on Cyber Expertise.

[83] Plexida, E. (2022). EU Dimensions of the 'Splinternet' Question. Centre for Global Cooperation Research.

[84] Tropina, T. (2022). Internet Fragmentation: What's at Stake? Centre for Global Cooperation Research.

[85] Woodward, M. (2021, July 8). 16 Countries with GDPR-like Data Privacy Laws. Retrieved from Security Scorecard.

[86] Reus-Smit, C. (2013, December). The concept of intervention. Review of International Studie, Special Issue: Intervention and the Ordering of the Modern World, pp. 1057-1076.

Based on this definition, policy and regulation documents from the E.U. will constitute a primary source for the analysis. Additional secondary literature, statements, expert opinions and even security blogs will be used to analyze the impact of E.U. interventions. The research for this thesis is literature review of both the E.U. documents directly from the E.U. website and using the snowball method for collecting expert opinions or other sources. Below in table 1 are the policies and regulations with the interventions that are covered in this thesis:

Document	**Description**	**Interventions**
The EU's Cybersecurity Strategy for the Digital Decade[87]	This new strategy aims to guarantee a global and open Internet with strong safeguards in the event of risks to the security and fundamental rights of citizens in Europe.	DNS4EU European Cyber Shield Joint Cyber Unit Cyber Diplomacy Toolbox Standardization Strategy
The Network and Information Security (NIS) 2 Directive	E.U.-wide legislation on cybersecurity	NIS2
Electronic identification and trust services for electronic transactions in the internal market and repealing Directive[88]	Provide the ability to identify E.U. citizens, residents and businesses.	eIDAS Regulation
Regulation on Privacy and Electronic Communications[89]	The ePrivacy legislation is an amendment to the General Data Protection Regulation (GDPR) on privacy with a focus on data processing.	ePrivacy Directive/Regulation
General Data Protection Regulation (GDPR)[90]	Privacy legislation for E.U. that gives individuals rights over their own data.	GDPR
Europe fit for the Digital Age[91]	A reform of the digital space that contains new rules for all digital services, e.g. social media and online market places.	Digital Markets Act Digital Service Act

[87] European Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[88] European Commission. (2022, June 16). The NIS2 Directive: A high common level of cybersecurity in the EU. Retrieved from europe.eu: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[89] European Commission. (2017, Januari 10). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[90] European Commission. (2016, April 27). General Data Protection Regulation. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[91] European Commission. (2020, December 15). Europe fit for the Digital Age: Commission proposes new rules for digital platforms. Retrieved from europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[92]	Introduction of a cybersecurity certification framework for the E.U.	Public-Private Partnerships Cybersecurity Certification Framework

Table 1: E.U. Policies and regulation, translated to interventions

Analysis will follow the next sequential steps to reach a conclusion for the main research question.

Step 1: Assess which interventions are impacting the technical layer.

Assess what the interventions from the E.U. documents are impacting the technical layer using the conceptualization of cyberspace[93]. This concept provides a scope of the technical layer but leaves some room for discussion. To supplement this concept, Werbach's four-layer model[94] will be used.

Step 2: Analyze these interventions.

In the second step we will dive into the interventions impacting the technical layer and analyze how they impact cyberspace on a technical level. This step is the basis for identifying if this impact introduces a form of borders as discussed in the theoretical framework.

Step 3: Analyze the impact on the borderless nature of cyberspace.

The final step is to identify if these impacts are also impacting the borderless nature of cyberspace and how. Using the identification of borders from chapter 3.2 allows us to cross-reference it with the interventions.

[92] European Commission. (2017, September 13). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

[93] Berg, J. v., Zoggel, J. v., Snels, M., Leeuwen, M. v., Boeke, S., Koppen, L. v., . . . Bos, T. d. (2015). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. NATO Science and Technology Organization.

[94] *Werbach, K. (2002). A Layered Model for Internet Policy. J. on Telecomm. & High Tech. L 37.*

5. Analysis

5.1. E.U. Interventions and the Conceptualization of Cyberspace

As mentioned in the framework for analysis in chapter 4.2 step 1, the Conceptualization of Cyberspace[95] with its three layers will be used as the model to plot the focus of different E.U. policies and regulations. This allows the identification of which E.U. documents are producing an intervention on the technical layer of cyberspace and potentially impact the borderless nature of cyberspace from there. The three-layer model leaves some room for interpretation when it comes to where the technical layer ends and the socio-technical layer begins. To complement the definition of the technical layer from the conceptualization of cyberspace, we will use the technical architecture described in chapter 3.1.4 as the content of the technical layer. If it is built on top of the Werbach's layered model[96], it is considered part of the socio-technical layer from the conceptualization of cyberspace. Werbach's model will also be the basis for the summary of interventions to identify any increased activity on specific areas within the technical layer.

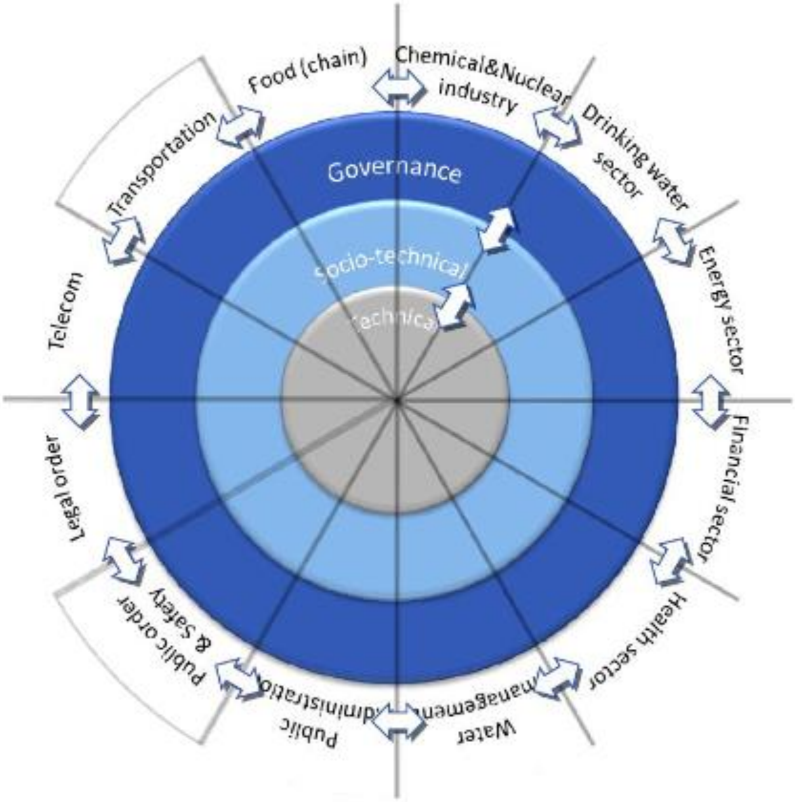


Figure 1: Conceptualization of Cyberspace: Three Layer Model[97]

[95] Berg, J. v., Zoggel, J. v., Snels, M., Leeuwen, M. v., Boeke, S., Koppen, L. v., . . . Bos, T. d. (2015). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. NATO Science and Technology Organization.

[96] *Werbach, K. (2002). A Layered Model for Internet Policy. J. on Telecomm. & High Tech. L 37.*

[97] Berg, J. v., Zoggel, J. v., Snels, M., Leeuwen, M. v., Boeke, S., Koppen, L. v., . . . Bos, T. d. (2015). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. NATO Science and Technology Organization.

Below we find an overview of the interventions. Even though the policies and regulations originate from the governance layer, as the E.U. develops them from a governance perspective, they can directly impact other layers. In the methodology we've identified the intervention that are covered in this thesis:

I.	DNS4EU	II.	European Cyber Shield
III.	Joint Cyber Unit	IV.	Cyber Diplomacy Toolbox
V.	Standardization Strategy	VI.	NIS2
VII.	eIDAS Regulation	VIII.	ePrivacy Directive/Regulation
IX.	GDPR	X.	Digital Markets Act
XI.	Digital Service Act	XII.	Public-Private Partnerships
XIII.	Cybersecurity Certification Framework		

Interventions can influence multiple layers; in that case we will analyze the specific section that impacts the technical layer in the next chapter. As the policies and regulations build heavily on cyberspace in general, they mostly do not target specific sectors. Therefore, sectors are left out of scope with this mapping. Below the interventions are mapped to their respective layers:

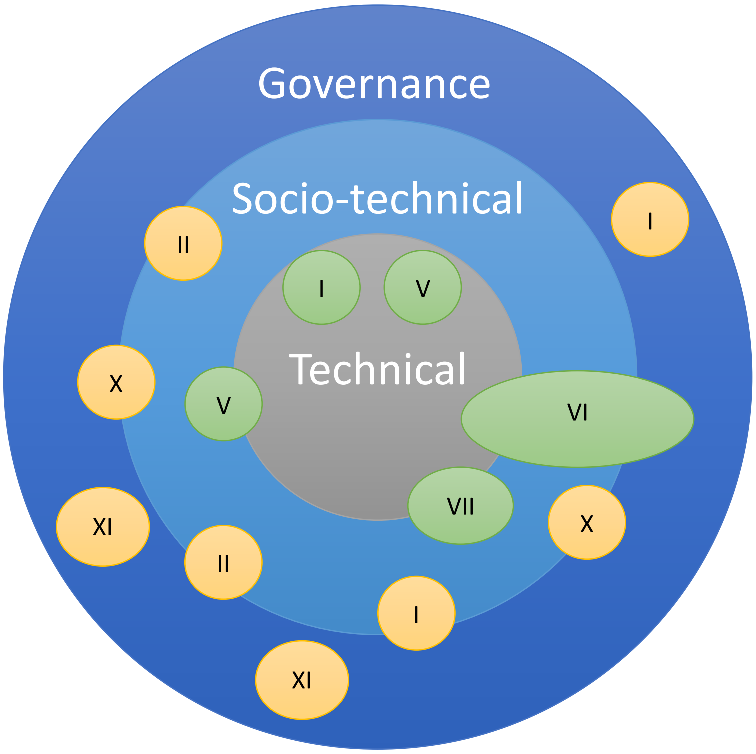


Figure 2: Interventions plotted to the Conceptualization of cyberspace in layers and (cyber) sub-domains.

5.2. E.U. Interventions on the Technical Layer

The E.U. is active on the technical layer by impacting the technical architecture of the Internet. In this chapter we will analyze the different interventions individually, the impact on the technical architecture and cyberspace's borderless nature. As the E.U. initiates interventions through proposals to allow feedback, we will include debate on the impact and how the E.U. handled feedback on their proposals.

5.2.1. DNS4EU

An European DNS resolver, more commonly known as DNS4EU[98]. DNS is one of the essential components for the Internet to operate as it allows users to visit websites through an URL instead of an IP address[99]. It aims to reduce the dependency and vulnerability of the E.U. from public DNS resolvers that are in the hands of just a few companies[100]. By doing so it should provide high reliability and enable protection against threats from cyberspace. According to the E.U. project overview it provides the following:

"DNS4EU shall offer a high level of resilience, global and EU-specific cybersecurity protection, data protection and privacy according to EU rules, ensure that DNS resolution data are processed in Europe and personal data are not monetized. It shall adhere to the latest internet security and privacy standards. It shall be widely discoverable and easy to configure by end-users on their equipment and software.

The service infrastructure shall offer additional optional services such as free parental control, as well as paid premium services for enhanced performance or security for corporate users."[101]

Impact on cyberspace's borderless nature

DNS resolvers are widely available nowadays and many Internet Service Providers (ISPs) provide their own. Most of the third-party DNS resolvers are provided by OpenDNS, Cloudflare and Google [102], all based in the US. The deployment of an E.U. based DNS provider of this type offers some balance. DNS4EU offers access to the global Internet as a public European service, adhering to European standards and security. This includes transparency with privacy by design, data protection and default standards, like GDPR[103]. One of the idea's behind DNS4EU is to counteract other models that are control-based and closed and instead facilitate the open and global Internet that is the expected of authority for the liberal sphere[104].

[98] European Commission. (2022, January 12). Backbone networks for pan-European cloud federation (CEF-DIG-2021-CLOUD). Retrieved from europa.eu: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

[99] Chapter 3.1.4

[100] Sar, E. V. (2022, January 19). The EU Wants Its Own DNS Resolver that Can Block 'Unlawful' Traffic. Retrieved from torrentfreak: https://torrentfreak.com/the-eu-wants-its-own-dns-resolver-that-can-block-unlawful-traffic-220119/

[101] European Commission. (2022, January 12). Backbone networks for pan-European cloud federation (CEF-DIG-2021-CLOUD). Retrieved from europa.eu: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

[102] Z, N. (2018, April 9). DNS Market Share Analysis — Identifying the Most Popular DNS providers. Retrieved from Medium: https://medium.com/@nykolas.z/dns-market-share-analysis-identifying-the-most-popular-dns-providers-80fefb2cfd05

[103] European Commission. (2020, October 15). Towards a next generation cloud for Europe. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

[104] European Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

As ICANN (The Internet Corporation for Assigned Names and Numbers) describes it *"Without the DNS, we wouldn't have a global, interoperable Internet"*[105]. We've seen how DNS facilitates a global interoperable Internet in chapter 3.1.4. For the most part the success of cyberspace lies in the inner workings of IP addresses and DNS. The fact that anyone at any place can open an URL and visit the intended website that is the same for all its users. The DNS, placed in the technical infrastructure of the Internet, provides this global consistency and creates the unity that we know today. IP addresses and DNS are at the technical level that know no borders[106], as all countries are ultimately connected to the same organization and root server that provide this global interoperability of the Internet. Because everything is connected to the same organization, the coordination of these universal frameworks happens through the multi-stakeholder model[107]. Without this approach it would be possible to remove a country from cyberspace more easily as one or multiple countries are in control. Removing or blocking users through DNS would implement a traditional border on a technical level as cyberspace does not function properly anymore for users from the blocked state. Such attempts have recently been made by Ukraine that requested Russia to be removed by ICANN from the Internet. This was rejected on the basis that ICANN does not control access to the Internet but only facilitates the global interoperability[108]. In ICANN's rejection it is specifically mentioned that this current implementation "*makes the Internet resilient against unilateral decision-making*".

A DNS resolver specifically from and for the E.U. raises the question of what unintended consequences it can have on cyberspace. Its impact on users should be minimal, following the proposal of the E.U.[109], as they are 'only' less susceptible to threats like phishing. In addition, there is the option for paid premium services, however, it is unknown what this entails exactly and therefore only leaves room for speculation. Since the DNS resolver is a government-run filtering and blocking tool, it brings the risk of censorship or collateral if websites are blocked without proper investigation. The implementation according to the proposal also includes filtering, read blocking, of 'illegal content', so anything with a court order can be blocked for all users in the region. This could also affect traffic running through the Internet's backbone that use the DNS resolver, these often operate without borders in mind and the impact can potentially result in blocking domains worldwide. The end state and technical setup of the DNS is not yet known, so we need to be careful when drawing conclusions here.

DNS4EU is a possible introduction of traditional borders applied to cyberspace[110]. The traditional borders provide governments control of the state's space, in this case, cyberspace. The ability for the E.U. to unilaterally decide how to handle DNS for its territory completely circumvents the current governance mechanism. The entire concept of global connectivity, which is also facilitated by DNS, is ensured through its multi-stakeholder model that blocks governmental geo-politics from impacting this connectivity. In

[105] ICANN. (2022, September 13). Understanding the Internet's Domain Name System. Retrieved from icann.org: https://www.icann.org/en/system/files/files/dns-infographic-13sep22-en.pdf

[106] Plexida, E. (2022). EU Dimensions of the 'Splinternet' Question. Centre for Global Cooperation Research.

[107] Internet Governance – Why the Multistakeholder Approach Works. (2016, April 26). Retrieved from Internet Society: https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

[108] Marby, G. (2022, March 2). marby-to-fedorov-02mar22. Retrieved from icann: https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[109] European Commission. (2022, January 12). Backbone networks for pan-European cloud federation (CEF-DIG-2021-CLOUD). Retrieved from europa.eu: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

[110] Plexida, E. (2022). EU Dimensions of the 'Splinternet' Question. Centre for Global Cooperation Research.

addition, it could introduce fragmentation on a technical level due to inconsistency in DNS answers after E.U. rules are applied to the DNS resolver. However, the E.U. values for cyberspace are open, free and interoperability. It can be argued that it is likely the E.U. will not compromise the global connectivity as it contradicts these values and the main goal of DNS4EU is to ensure a more resilient and secure cyberspace for its users. Taking this into consideration it is likely that the E.U. will provide a DNS service and only block specific cyber threats without using the service for geo-politics. Therefore, not fragmenting the Internet.

5.2.2. Standardization Strategy

Standards and standardization are of global importance. Activity on setting or influencing standards are increasing in other regions of the world and in response the E.U. wants to do the same[111]. At the international level the E.U. wants to promote and defends its vision of cyberspace. Through its standardization strategy and amendment to the Regulation on standardization the E.U. wants to strengthen its global competitiveness and instill its democratic values in technology applications. This standardization strategy consists of five key sets of actions[112]:

1. Anticipate, prioritize and address standardization needs in strategic areas;
2. Improve the governance and integrity of the European standardization system;
3. Enhance European leadership in global standards;
4. Support innovation;
5. Enable the next generation of standardization experts.

Through this approach the E.U. is adapting its leadership on standards in cyberspace to better align with the volatility of everything that’s happening[113].

Impact on cyberspace’s borderless nature

Daniel Benolielt describes standards as *“a common and repeated use of rules, conditions, guidelines or characteristics that serves to measure products, related processes, and production methods”*[114]. The development of new digital technologies is happening fast and these require international standards to ensure the continuous interoperability of technical architecture of the Internet. New technologies include AI, quantum computing and infrastructures like 5G that impact all layers of cyberspace and thus also become part of the technical layer. Ensuring standardization at an early stage leads to better interoperability once deployed and globally adopted.

Next to completely new technologies there are also updates or upgrades of existing standards. Internationally there are states trying to push new standards that represent their political and ideological

[111] European Commission. (2022, February 2). New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market. Retrieved from europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

[112] European Commission. (2022, February 2). New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market. Retrieved from europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

[113] European Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[114] Benolielt, D. (2004). echnological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology. California Law Review, pp. 1069-1116.

agenda[115]. An example is Huawei's, China's state-owned telecom giant, proposal for a "New IP"[116]. Following this proposal there has been debate on potential fragmentation[117], as it could replace the existing Internet standards. So far New IP isn't at the stage that this might happen, but it illustrates the presence of other states from the sovereign authoritarian sphere that are actively trying to influence international standards. These political and ideological agendas often do not correspond with the global, open and transparent vision the E.U., as a liberal authority sphere, has for cyberspace. This is embedded in the E.U. strategy: *"Shaping international standards in the areas of emerging technologies and the core internet architecture in line with EU values is essential to ensure that the Internet remains global and open, that technologies are human-centric, privacy-focused, and that their use is lawful, safe and ethical."*[118].

E.U.'s approach for achieving this strategy is a more active partnership with organizations that develop these standards, primarily the International Organization for Standardization (ISO), the International Telecommunication Union (ITU) and the International Electronical Commission (IEC). But the global partnerships are not limited to these three organizations[119]. In addition, the E.U. wants to improve its coordination between Member States, stakeholders and national standardization bodies to increase its influence further in global standardization. The newly established E.U. Excellence hub on standards in the selected organization to monitor and coordinate standardization activities[120]. Global adoption of these standards are high on the agenda and will continue its dialogue with states from the sovereign authority sphere to explore possible areas of cooperation. With this strategy they want to be more agile and fast in the development of standards in order to ensure E.U. cyberspace values remain dominant.

The idea behind this intervention is not to directly impact cyberspace's borderless nature, but rather impact it by maintaining it as is. It is argued that the Internet is based on trust, trusting that the same 'language' is spoken by using the same standards and protocols, and different stakeholders have influence through the multi-stakeholder governance model[121]. This model ensures that there is trust in the structure and workings of the Internet but circumventing this model can break trust. Especially on a technical level this is important if it wants to maintain its interoperability. In the strategy itself the E.U. also emphasizes the key role of the multi-stakeholder model and the desire to strengthen it[122]. However, it is of vital importance that the E.U. follow this model on proposals that directly impact the technical layer. In the past the E.U. has published

[115] European Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[116] Durand, A. (2020, October 27). New IP. Retrieved from ICANN: https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf

[117] Nanni, R. (2022). The 'China' Question in Internet Fragmentation: Evidence From the 'New IP' Fragmentation: Evidence From the 'New IP'. Centre for Global Cooperation Research.

[118] European Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[119] European Commission. (2022, February 2). An EU Strategy on Standardisation. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031

[120] European Commission. (2022, February 2). An EU Strategy on Standardisation. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031

[121] Antonijevic, S. (2019, January). The internet: A brief history based on trust. SOCIOLOGIJA, pp. 464-477. doi:10.2298/SOC1904464A

[122] European Commission. (2022, February 2). An EU Strategy on Standardisation. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031

interventions, like the NIS2 Directive that we will cover in chapter 5.2.5, that impact the technical layer and did not follow the multi-stakeholder model[123].

Let's hope the E.U. learned from its choice of bypassing the multi-stakeholder model, which is likely with the publication of the standardization strategy that includes the strengthening the cooperation. This way the E.U. uses all available knowledge when drafting policy that impacts the technical layer. If the E.U. properly follows their strategy it will have significant impact on cyberspace's borderless nature by counter influencing states that desire more sovereignty on cyberspace[124]. The strengthening of E.U. influence on the entire technical architecture through standards and its standardization process leads to higher likelihood of an open, free and interoperable cyberspace. In short, the Internet will keep its global connectivity and avoid fragmentation.

5.2.3. eIDAS 2.0

eIDAS stands for electronic IDentification, Authentication and Trust Services. It is a regulation developed for electronic identification and electronic transactions through trust services for the E.U. market[125]. Fundamentally it should provide identification and authentication, therefore the eIDAS regulation defines its schemes on this as part of a common electronic identity, also as part of the European Digital Identity[126].

eIDAS 2.0 is an update to its predecessor that contained an identity framework that will enable a set of digital identity credentials for European citizens that are recognized anywhere in the E.U.[127] This regulation is to increase the cooperation between different services offered, especially present between public and private services. The cooperation has a need for a simpler connection method, which eIDAS should provide. For now, the regulation does not yet define if this cooperation between public and private services will be a simple recommendation or an actual legal obligation. In addition, the regulation aims to provide extra services and this is the impact on the technical layer. One of the objectives of this update is to offer new authentication methods by creating a unified and secure identification service[128].

Impact on cyberspace's borderless nature

The proposed method for this new service is through Qualified Web Authentication Certificates (QWAC's). This should provide, according to the proposed amendment, the following: *"web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user-friendly manner."*[129]. The E.U. mandates browsers to accept Certificate Authorities (CAs) from E.U. member states. These QWACs are

[123] Dawson, C. (2022, May 11). NIS2 Directive Article 23 Will Lead to Inconsistencies and Conflicts Within the Domain Name Industry. Retrieved from CircleID: https://circleid.com/posts/20220511-nis2-directive-article-23-will-lead-to-inconsistencies-and-conflicts-within-the-domain-name-industry

[124] Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020, 07 01). Authority conflicts in internet governance: Liberals vs. sovereigntists? Cambridge University Press, pp. 364 - 386. doi:10.1017/S2045381720000167

[125] European Commission. (2021, June 3). establishing a framework for a European Digital Identity. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[126] European Commission. (n.d.). European Digital Identity. Retrieved from europa.eu: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[127] European Commission. (2022, June 16). The NIS2 Directive: A high common level of cybersecurity in the EU. Retrieved from europe.eu: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[128] European Commission. (2021, June 3). establishing a framework for a European Digital Identity. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[129] European Commission. (2021, May 28). A trusted and secure European e-ID - Regulation. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

developed by the European Telecommunications Standards Institute (ETSI)[130]. These QWACs have similar functionality as existing certifications validation options and these options have proven to not bring the level of security expected[131]. In fact the opposite occurs as it is possible for malicious websites to obtain validated certificates, leading its visitors to assume they are on a safe website. As a result, it introduces lower security in cyberspace for its users[132].

Introducing a form of digital identity supported by the government itself for the E.U. leads to the belief a traditional border is implemented, similarly to E.U. passports. On the specific aspects of QWACs it requires all web browsers to recognize E.U. certificates, logically leading to near global recognition. As a result, it can be argued that traditional borders are not introduced as cyberspace users from the E.U. can still access the Internet using a browser. As a matter of fact, the intervention only states the browser need to recognize it and likely only faces fines if the browser does not. This intervention is more towards the content layer of Werbach's model and does impact the standards and protocols that facilitate the global connectivity.

5.2.4. ePrivacy Directive/Regulation

First introduced in 2002 and amended in 2009, the ePrivacy Directive (EPD), more commonly known as the 'cookie law'[133]. It received its nickname after the explosion of consent requests through pop-ups after it came into effect, to the point that users even find it to be annoying. It works with the GDPR by supplementing it by addressing the tracking of users, confidentiality of electronic communications concerns and processing of personal data from visitors inside the E.U.[134]. It was the first legislation that regulated the use of cookies and trackers and introduced a mandatory consent before installing them[135]. Together with the GDPR it forms the data privacy regime in Europe with an extraterritorial scope, this means that any website must comply if it has visitors from the E.U.

Europe has successfully achieved the Brussels Effect[136] with the ePrivacy Directive and GDPR as other states have followed by implementing similar data privacy laws, e.g., South Africa's POPIA[137] and Brazils LGPD[138].

[130] European Commission. (2021, June 3). establishing a framework for a European Digital Identity. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[131] Saltaformaggio, B., & Konte, M. (2019, June 28). Understanding the Role of Extended Validation Certificates in Internet Abuse.

[132] Hancock, A., & Callas, J. (2022, February 9). What the Duck? Why an EU Proposal to Require "QWACs" Will Hurt Internet Security. Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks/2022/02/what-duck-why-eu-proposal-require-qwacs-will-hurt-internet-security

[133] European Commission. (2017, Januari 10). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[134] Koch, R. (n.d.). Cookies, the GDPR, and the ePrivacy Directive. Retrieved from gdpr.eu: https://gdpr.eu/cookies/

[135] EU cookie law | ePrivacy Directive and cookies. (2021, December 21). Retrieved from Cookiebot: https://www.cookiebot.com/en/cookie-law/

[136] Bradford, A. (2012). The Brussels Effect. Columbia Law School.

[137] Protection of Personal Information Act (POPI Act). (n.d.). Retrieved from POPIA: https://popia.co.za/

[138] Advogados, R. P. (2020, October). Brazilian General Data Protection Law (LGPD, English translation). Retrieved from IAPP: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

Adding to the Brussels Effect, a 2021 study by Cisco shows that data privacy is becoming a consumer demand with 79%[139] saying it's a buyer factor for them.

In 2017 the ePrivacy Directive received a proposal in draft that is meant to replace it by the ePrivacy Regulation (EPR), which built on the EPD and expands its definitions. The EPR was supposed to come into effect in together with the GDPR but missed that goal. The main difference between these two is that a directive must be incorporated into national law whereas regulation becomes legally binding the moment it comes into effect. EPR adds on the EPD by addressing browser fingerprinting in a similar way as its cookie approach, it includes metadata protection and incorporate new communication techniques[140].

Impact on cyberspace's borderless nature

These communication techniques make no distinction when it comes to machine-to-machine communications, meaning it identifies smartwatches similarly to a water quality sensor. As a result, they all need to adhere to the ePrivacy Regulation and obtain the user's consent for processing of data, including metadata. This would not be feasible according to Nick Wallece[141] as it means users must consent to data processing for every new network it connects to as it tries to exchange data with road sensors when using live traffic data. This analysis is supported by studies on the impact of ePrivacy[142] as it impacts the actual routing of the Internet by not automatically allowing it to choose the best available route. This implementation would significantly impact cyberspace by tampering with its routing process, as it would require continuous contact with the user because of changes on a technical level. As a result, the Internet would still work for its users, but would be nearly unusable due to consent requests for all the metadata processing and cookies. Theoretically this would only apply to users from the E.U., but on a technical level it would be hard to distinguish the users. It is possible to use geo-location based on IP addresses to identify where users are likely connecting from[143]. However, with the risk of administrative fines from the EPR it is likely that the underlying infrastructure applies the cookie consent request to all users[144].

The impact of this intervention traveled all the way down to the physical layer of Werbach's model, because of the inclusion of sensors and other physical infrastructure[145]. Though it was not introducing forms of incompatibility on any layer, tampering with the routing process reduces it usability[146]. As soon as it was discovered this, apparently unintended, consequence was corrected by updating the E.U. proposal[147]. With this update it is allowed to process metadata for the purpose of network management or network

[139] Building Consumer Confidence Through Transparency and Control. (2021). Retrieved from CISCO: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf?CCID=cc000742&DTID=esootr000875&OID=rptsc027438

[140] Church, P. (2017, June 6). EU - Status of the proposed ePrivacy Regulation: Tighter cookie rules and more. Retrieved from Linklaters.

[141] Wallace, N. (2018, March 13). EU e-privacy proposal risks breaking 'Internet of Things'. Retrieved from EU Observer.

[142] Niko Härting / Patrick Gössling*Study on the Impact of the Proposed Draft of the ePriv-acy-Regulation

[143] . "Imagine there's no countries..." – Geo-identification, the law and the not so borderless Internet∗ Dr. Dan Jerker B. Svantesson∗∗

[144] Wallace, N. (2018, March 13). EU e-privacy proposal risks breaking 'Internet of Things'. Retrieved from EU Observer.

[145] *Werbach, K. (2002). A Layered Model for Internet Policy. J. on Telecomm. & High Tech. L 37.*

[146] Niko Härting / Patrick Gössling*Study on the Impact of the Proposed Draft of the ePriv-acy-Regulation

[147] European Commission. (2022, June 7). Proposal for an ePrivacy Regulation. Retrieved from europa.eu.

optimization[148]. Unintentionally impacting the technical layer of cyberspace is always a risk when drafting legislation, especially when it is still in proposal form. The fact that the E.U. updated its proposal to ensure optimal global connectivity demonstrates how important it find its values for cyberspace.

5.2.5. NIS2 Directive

The Networks and Information Security Directive (NIS) is receiving an update to NIS2. It is an E.U. wide legislation on cybersecurity and includes legal measures to further the overall level of cybersecurity[149]. It includes different types of interventions on the government layer and socio-technical layer, like the requirement of a national Cyber Security Incident Response Teams (CSIRTs), setup collaboration between CSIRTS, implement measures for vital sectors of the economy and introduce legal measures. It seeks to respond to the cybersecurity threat landscape, that is changing rapidly. The main objective is to build a more resilient Europe through the protection of vulnerable sectors and increase the cooperation between Member States' cybersecurity mechanisms[150]. Members States will need to develop national laws to follow this E.U. directive. The NIS2 is a rather large document with many interventions. For this analysis we will only focus on the section that impacts the technical layer of cyberspace directly as that is the research for this thesis. These interventions are on the DNS and trust service providers.

Impact on cyberspace's borderless nature

That the role of DNS is vitally important for cyberspace is clear from the DNS4EU analysis. In the initial NIS2 proposal all providers of DNS services along the DNS resolution chain are moved into scope of the directive, including root operators of root name services, top-level domain name servers and authoritative name servers for domain names and recursive resolvers[151]. Article 4(14) describes DNS service provider as follows: ***"'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers."***[152]

As a result, all providers of DNS services need to adhere to E.U. regulation or face administrative fines[153]. This led to high debate around the world due to the technical implications that could follow. According to Callum Voge from the Internet Society[154] it can have an impact on critical properties of the Internet's way of working[155]. NIS2 introduces new obligations for DNS service providers that already have existing obligations from the community, or multi stakeholders, governance structure. It runs the risk of adding

[148] The EU ePrivacy Regulation (ePR). (n.d.). Retrieved from IT Governance.

[149] European Commission. (2022, June 16). The NIS2 Directive: A high common level of cybersecurity in the EU. Retrieved from europe.eu: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[150] European Commission. (2022, June 16). The NIS2 Directive: A high common level of cybersecurity in the EU. Retrieved from europe.eu: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.pdf

[151] Voge, C., Kolkman, O., & Robachevsky, A. (2021, October 11). Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021. Retrieved from Internet Society.

[152] European Commission. (2022, June 16). The NIS2 Directive: A high common level of cybersecurity in the EU. Retrieved from europe.eu: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[153] Bruder, A. H., Simon, D. A., Randall, R., & Yaros, O. (2022). NIS2 Directive New Cybersecurity Rules Expected in the EU. Retrieved from Mayer Brown.

[154] Voge, C., Kolkman, O., & Robachevsky, A. (2021, October 11). Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021. Retrieved from Internet Society.

[155] The Internet Way of Networking: Defining the critical properties of the Internet. (2020, September 9). Retrieved from Internet Society.

different layers of accountability and obligations that are not aligned. For example, the potential differences between local community set requirements versus governmental set requirements, where it is expected that the governments requirements will be followed due to potential fines. This reduces the autonomy of the service and potentially even the resilience of the Internet[156].

Olaf Kolkman published an analysis that shows an even greater impact of the NIS2 Directive through a possible the introduction of fragmentation[157]. The additional requirements on DNS services can mean that entities are ordered to "cease non-compliant conduct" by Member States, resulting in the "disintegration of common global identifiers and contributes to Internet fragmentation"[158]. Providers might also try to avoid fines and change their behavior, even to the extent of blocking European DNS queries. A similar situation happened before with the GDPR where European readers were blocked from viewing U.S. news sites[159].

Debate on the NIS2 even went to the point where the Internet Society said the following: "… would harm multistakeholder processes and contribute to the disintegration of common global identifiers. Furthermore, it runs contrary to the EU's historic support of a 'single, open, neutral, free, secure and un-fragmented network'"[160]. The bypassing of the multi-stakeholder process is mentioned by several cyber experts like Christiaan Dawson[161], who emphasis the fact that this process was designed to ensure global interoperability and avoid conflicting requirements.

All the debate that followed the NIS2 proposal publication stems from the expanded scope that included the root zone servers. These top-level Root Server Operators are mostly operating from outside of the E.U., e.g., the U.S. Department of Defense or NASA. Imposing NIS2 regulations that include random audits would lead to distrust between essentially the Internet and the E.U.[162]. As we've discussed before, on the technical layer the Internet works on trust[163]. Which means the inclusion of the root servers would actually work against it. It would also result in the impression that the E.U. wants to regulate the whole Internet by imposing its control on the DNS, a critical part of the inner workings of cyberspace[164]. While this in itself

[156] Voge, C., Kolkman, O., & Robachevsky, A. (2021, October 11). Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021. Retrieved from Internet Society.

[157] Kolkman, O. (2021, November 5). NIS2 – Security, Resiliency, and DNS server infrastructure. Retrieved from Internet Society.

[158] Voge, C., Kolkman, O., & Robachevsky, A. (2021, October 11). Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021. Retrieved from Internet Society.

[159] European readers still blocked from some US news sites. (2018, June 26). Retrieved from BBC News.

[160] Voge, C., Kolkman, O., & Robachevsky, A. (2021, October 11). Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021. Retrieved from Internet Society.

[161] Dawson, C. (2022, May 11). NIS2 Directive Article 23 Will Lead to Inconsistencies and Conflicts Within the Domain Name Industry. Retrieved from CircleID: https://circleid.com/posts/20220511-nis2-directive-article-23-will-lead-to-inconsistencies-and-conflicts-within-the-domain-name-industry

[162] Hubert, B. (2021, May 10). Dear EU: Please Don't Ruin the Root. Retrieved from berthub.

[163] Antonijevic, S. (2019, January). The internet: A brief history based on trust. SOCIOLOGIJA, pp. 464-477. doi:10.2298/SOC1904464A

[164] Hubert, B. (2021, May 10). Dear EU: Please Don't Ruin the Root. Retrieved from berthub.

might feel to not impact cyberspace too heavily as the E.U. values correspond to its current workings, it does allow other governments with desire to control cyberspace to try and follow[165].

Official feedback on the NIS2 proposal was submitted in the months following its publication. Organizations like ICANN[166], RIPE[167] and I2Coalition[168] requested the root server operators were to be removed from the NIS2 scope to address the concerns of the community.

"Root name servers should be out of scope; regulating them is contrary to the EU's vision of a "single, open, neutral, free, secure and un-fragmented network" and could encourage and empower states advocating for a top-down, state-controlled Internet governance approach, instead of the multi-stakeholder approach."

RIPE: NCC Response to NIS 2 Directive[169]*.*

Initially experts deemed it unlikely that the regulation would be adjusted as it was moving towards the final stages of negotiation[170]. Fortunately, the problem was understood by the E.U. and fully removed the root zone from scope before adopting the new directive[171]. The change of scope demonstrates again the desire of E.U. to uphold its values for cyberspace. Developing policy to provide a safer cyberspace for its users is challenging and can result in unintended consequences[172]. It is all about finding a balance between a level of digital sovereignty and the cyberspace we know today with its ever-increasing cyber threats.

[165] Ignatius, D. (2021, May 4). Russias Plot Control Internet is no longer Secret. Retrieved from The Washington Post.

[166] ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive). (2021, March 19). Retrieved from ICANN.

[167] RIPE NCC Response to the European Commission's Proposed NIS 2 Directive. (2021, March). Retrieved from RIPE NCC.

[168] Dawson, C. (2022, May 11). NIS2 Directive Article 23 Will Lead to Inconsistencies and Conflicts Within the Domain Name Industry. Retrieved from CircleID: https://circleid.com/posts/20220511-nis2-directive-article-23-will-lead-to-inconsistencies-and-conflicts-within-the-domain-name-industry

[169] RIPE NCC Response to the European Commission's Proposed NIS 2 Directive. (2021, March). Retrieved from RIPE NCC.

[170] Kolkman, O. (2021, December 17). NIS2 Inconsistency – a DNS Supply Chain Perspective. Retrieved from Internet Society.

[171] Bertuzzi, L. (2021, October 28). EU Parliament committee adopts new cybersecurity law for critical services. Retrieved from EURACTIV.

[172] Hubert, B. (2021, May 10). Dear EU: Please Don't Ruin the Root. Retrieved from berthub.

5.3. Summary of interventions on the technical layer according to Werbach's model

The E.U. is quite active when it comes to developing methods to govern cyberspace in one way or another as we've seen in chapter 5.1. To get a complete picture of the impact of the E.U. we will include Werbach's Layered Model for Internet Policy used for describing the Internet's infrastructure. All interventions impact at least one of the layers, but this insight provides where the E.U. is most active. Analyzing will be done from the bottom up as the layers are stacked on top of each other.

5.3.1. Physical layer

On the physical layer of Werbach's model the E.U. is least active when it comes to the identified interventions. Its standardization strategy is impacting every layer, thus including this one. It needs to ensure the interoperability of new technologies like 5G so the same specifications can be used globally. However, because the following layers are developed with interoperability in mind it is less impactful to ensure standardization on the physical layer. Any interventions from the E.U. to alter the physical infrastructure by either boosting or breaking it have not been identified.

5.3.2. Logical layer

The logical layer that facilitates the Internet with its core TCP/IP protocols. It's the layer that allows for the interconnection between physically transferring the data and its users. As Konstantinos Komaitis says: "the glue that holds it together as one global and open network"[173]. E.U. is active on this layer with ensuring the protocols continue to work for an open and interoperable Internet through their standardization strategy. It is where they will challenge new proposals like Huawai's "New IP" if it jeopardizes E.U. values. The desire to maintain an E.U. values for cyberspace is thus instilled that the E.U. is willing to reform proposals to ensure that this will not be compromised. A recent intervention that demonstrates this is the reform of the Cookie Law to avoid tempering with the Internet's routing.

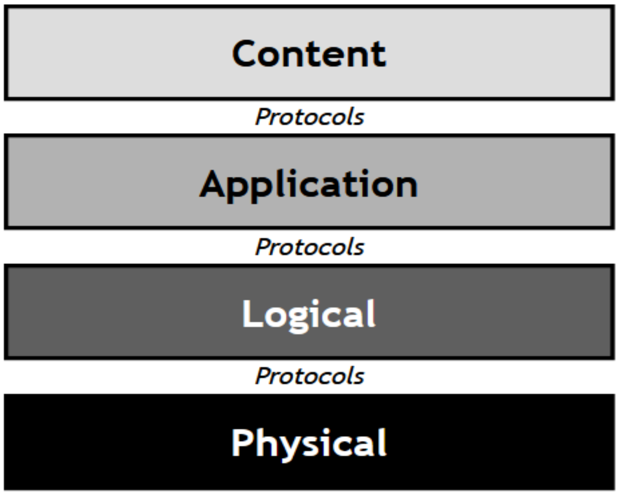


Figure 3: Werbach's Layered Model for Internet Policy

5.3.3. Application layer

The E.U. is actively proposing and implementing interventions that impact the Internet's architecture on the application layer. From chapter 3.1.4 that describes the architecture we've seen that one of the main protocols on this layer is DNS. The analysis of E.U. interventions, specifically NIS2 and DNS4EU, show the impact on this specific protocol and its service providers. The Application layer is the layer that allows users to interact with cyberspace the way they are used to. To highlight the importance of this layer for, a quote from the service provider of IP addresses, ICANN: *"without the DNS, we wouldn't have a global interoperable*

[173] Komaitis, K. (2022, December 9). Europe's Risky Plan for the Internet. Retrieved from directionsblog.eu.

Internet" [174]. This is the reason the E.U. wants to implement their interventions to ensure a stable DNS service for users from the E.U., but might introduce negative effects like the withdrawal of other DNS service providers or blocking of E.U. IP addresses outside of the E.U. In addition, the E.U. is also active on this layer through their standardization strategy as it impacts every layer in a similar fashion. Interventions from the E.U. on this layer can inadvertently impact the borderless nature of cyberspace like DNS4EU.

5.3.4. Content layer

On the content layer of the Internet's architecture, we expect interventions that impact user applications, like the example from thingiverse in chapter 3.1.4. eIDAS's impact on this layer is through the introduction of a public identification mechanism for E.U. citizens. We've seen that the impact is potentially lowering the Internet's security level through the introduction of QWACs because of its unilateral development by the European Telecommunications Standards Institute (ETSI). Though impacting cyberspace in general, there is no impact expected on its borderless nature.

[174] ICANN. (2022, September 13). Understanding the Internet's Domain Name System. Retrieved from icann.org: https://www.icann.org/en/system/files/files/dns-infographic-13sep22-en.pdf

Conclusion

The Internet is successful thanks to its use of technology, the way it operates and how it evolves. It provides opportunities for an online environment that allows users to connect, share, learn and innovate. The general design of the Internet was not built for a specific purpose, but rather a strong foundation to allow a wide variety of applications to flourish. This means the technical infrastructure needs to remain open and speak a common language, in this case through standards and protocols. Using these standards and protocols as geopolitical agendas can endanger the nature of the Internet. Smiljana Antonijevic states the Internet is based on trust, not necessarily on the socio-technical layer that includes a debate on types of interactions, but on a technical layer the Internet "just works"[175]. People trust the Internet to just work because today everyone uses the same underlying technical infrastructure. Especially the TCP/IP and DNS are the foundation on which cyberspace thrives.

Incompatible standards and protocols can be introduced through different types of interventions, even if it is unintentional. Equally important, if the multistakeholder governance structure of the Internet is challenged or circumvented through national law and regulation we risk introducing fragmentation. Elena Plexida argues that the standards, protocols and its governance structure are the glue that holds the Internet together[176]. Without these functions the Internet would break and no longer 'just work'.

After analyzing the interventions proposed, implemented or reformed by the E.U. and reviewing different documentation, we have a good understanding of how the E.U. is impacting the borderless nature of cyberspace. In this thesis, we zoomed in on the fact that the Internet is considered borderless through its technical architecture and identified how borders work, or not work, in cyberspace.

The E.U. is introducing a form of traditional borders on a technical level through their interventions like DNS4EU. Of course, with the good intentions of making cyberspace a safer and resilient environment for its E.U. users, but also with the risk of creating censorship. It is likely that the impact is not going to be significant on the borderless nature of cyberspace, because of the values E.U. has for cyberspace. After all they are the opposite of the sovereign authority sphere that desires complete control over 'its' cyberspace. Instead, the E.U. is part of the liberal authority sphere that wants to maintain it as open, free and interoperable. This can directly be seen when the E.U. introduces an intervention that impacts these values, like the ePrivacy Regulation. The Internet could have fragmented and the E.U. actually reformed its proposal to ensure the E.U. values are maintained. On the other hand, a similar situation happened with the NIS2 Directive, which bypassed the multi-stakeholder model and introduces an impact on the global DNS. This legislation is not yet finalized, so any outcome will solidify or break the trust in the multi-stakeholder model. To an extent it looks like attempts were made to force the Brussels Effect on the technical layer by this unilateral development of policy. According to academia the E.U. should only focus on the layers that build on top of the technical layer[177].

So far, the E.U. has had a limited impact with its interventions on the borderless nature of cyberspace, but the opposite can be expected for the future. Standardization impacts every layer of the technical

[175] Antonijevic, S. (2019, January). The internet: A brief history based on trust. SOCIOLOGIJA, pp. 464-477. doi:10.2298/SOC1904464A

[176] Plexida, E. (2022). EU Dimensions of the 'Splinternet' Question. Centre for Global Cooperation Research.

[177] Plexida, E. (2022). EU Dimensions of the 'Splinternet' Question. Centre for Global Cooperation Research.

architecture can be influenced by both spheres of authority. Here is where the biggest impact of the E.U. is likely to occur with its standardization strategy. With the E.U. strengthening its relations and contribution to the standardization process and following the multi-stakeholder model the E.U. can influence the technical layer of cyberspace to stay as we know today. Here it is of vital importance that the E.U. also follows this process with their own proposals that impact the technical layer. There might be policies and legislation on top that apply forms of border, like the GDPR, but technically the Internet will continue to be one giant network.

Reflection

The research focuses on governance measures and interventions from the E.U. It does not include non-governmental organizations that impact cyberspace while residing within the E.U or anything outside of the E.U. As a result, it scratches the surface on what is happening in cyberspace in relation to its borderless nature. It does provide an insight into what is happening within the E.U. and how this might affect or even steer globally. Regarding the extent of which the interventions are implemented, or likely to be implemented, also leaves room for further analysis.

Using the conceptualization of cyberspace, it is understood that changes through interventions and other means are happening on layers other than the technical layer. It is entirely possible that these changes can impact the borderless nature of cyberspace, but this is likely through non-technical means or indirectly impacting the technical layer. For example, socio-technical influences are not considered like language or psychology.

Recommendations for Future Research

The primary focus of this thesis was on governance interventions that are on the technical level of cyberspace, as discussed in chapter 4. How the E.U. impacts cyberspace through their interventions can be expended to the entirety of cyberspace, leading to the analysis of the socio-technical layer and the governance layer. This will provide a more holistic view of the impact of the E.U. on cyberspace, these interventions might also affect the technical layer of cyberspace through other means. Future research on these layers in recommended.

Cyberspace can be impacted by non-governmental organizations, individual states or individuals. These impacts through interventions can be aligned with the E.U.'s vision of cyberspace or oppose it. Analyzing the interventions of these other entities can provide insight into the views within the E.U. on how cyberspace is and should be governed.

The final recommendation is the analysis of other large players in cyberspace. In this research we've focused on a government from the liberal authority sphere, but there are others in this sphere. Are they sharing the vision E.U. has for cyberspace and do they support it in a similar fashion? Logically there are governments that do not align with these views and values, as discussed these are part of the sovereign authority sphere. It would be valuable to have insights in how these governments impact cyberspace on each of the layers from the three-layer model used in this research.

Bibliography

Advogados, R. P. (2020, October). *Brazilian General Data Protection Law (LGPD, English translation)*. Retrieved from IAPP: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

Antonijevic, S. (2019, January). The internet: A brief history based on trust. *SOCIOLOGIJA*, pp. 464-477. doi:10.2298/SOC1904464A

Bailey, J. (2004). *Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation.* Manitoba Law Journal Vol 30 No 2.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). Securitization' Revisited: Theory and Cases. *International Relations*, pp. 494-531.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Davos, Switzerland.

Benolielt, D. (2004). echnological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology. *California Law Review*, pp. 1069-1116.

Berg, J. v., Zoggel, J. v., Snels, M., Leeuwen, M. v., Boeke, S., Koppen, L. v., . . . Bos, T. d. (2015). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *NATO Science and Technology Organization*.

Bertuzzi, L. (2021, October 28). *EU Parliament committee adopts new cybersecurity law for critical services*. Retrieved from EURACTIV.

Betz, D. J., & Stevens, T. (2011, November 30). Cyberspace and the State: Chapter One: Power and cyberspace. pp. 35-54. doi:10.1080/19445571.2011.636954

Border. (n.d.). Retrieved from National Geographic: https://education.nationalgeographic.org/resource/border

Bradford, A. (2012). The Brussels Effect. *Columbia Law School*.

Brate, A. (2002). Techno Manifestos.

Brill, J. (2018, May 21). *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data.* Retrieved from Microsoft: https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/

Bruder, A. H., Simon, D. A., Randall, R., & Yaros, O. (2022). *NIS2 Directive New Cybersecurity Rules Expected in the EU*. Retrieved from Mayer Brown.

Building Consumer Confidence Through Transparency and Control. (2021). Retrieved from CISCO: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf?CCID=cc000742&DTID=esootr000875&OID=rptsc027438

Buzan, B. G., Waever, O., & de Wilde, J. H. (1998). Security: A New Framework for Analysis. *Lynne Rienner*, p. 247.

Church, P. (2017, June 6). *EU - Status of the proposed ePrivacy Regulation: Tighter cookie rules and more*. Retrieved from Linklaters.

Claessen, E. (2020). Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. (5.1). Journal of Cyber Policy. doi:I: 10.1080/23738871.2020.1728356

Dawson, C. (2022, May 11). *NIS2 Directive Article 23 Will Lead to Inconsistencies and Conflicts Within the Domain Name Industry*. Retrieved from CircleID: https://circleid.com/posts/20220511-nis2-directive-article-23-will-lead-to-inconsistencies-and-conflicts-within-the-domain-name-industry

DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). Internet Fragmentation: An Overview. *Davos: World Economic Forum*.

Durand, A. (2020, October 27). *New IP.* Retrieved from ICANN: https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf

Egan, E., & Beringer, A. (2018, April 17). *Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live.* Retrieved from Meta: https://about.fb.com/news/2018/04/new-privacy-protections/

EU cookie law | ePrivacy Directive and cookies. (2021, December 21). Retrieved from Cookiebot: https://www.cookiebot.com/en/cookie-law/

European Commission. (2016, April 27). *General Data Protection Regulation*. Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Commission. (2017, Januari 10). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.* Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

European Commission. (2017, September 13). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

European Commission. (2020, December 15). *Europe fit for the Digital Age: Commission proposes new rules for digital platforms*. Retrieved from europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

European Commission. (2020, December 16). *The EU's Cybersecurity Strategy for the Digital Decade.* Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2020, October 15). *Towards a next generation cloud for Europe*. Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

European Commission. (2021, May 28). *A trusted and secure European e-ID - Regulation.* Retrieved from europa.eu: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

European Commission. (2021, June 3). *establishing a framework for a European Digital Identity.* Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

European Commission. (2022, February 2). *An EU Strategy on Standardisation.* Retrieved from europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031

European Commission. (2022, January 12). *Backbone networks for pan-European cloud federation (CEF-DIG-2021-CLOUD)*. Retrieved from europa.eu: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

European Commission. (2022, February 2). *New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market*. Retrieved from europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

European Commission. (2022, June 7). *Proposal for an ePrivacy Regulation*. Retrieved from europa.eu.

European Commission. (2022, June 16). *The NIS2 Directive: A high common level of cybersecurity in the EU.* Retrieved from europe.eu: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

European Commission. (n.d.). *European Digital Identity*. Retrieved from europa.eu: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

European Commission. (n.d.). Territorial status of EU countries and certain territories. Retrieved from https://taxation-customs.ec.europa.eu/territorial-status-eu-countries-and-certain-territories_en

European readers still blocked from some US news sites. (2018, June 26). Retrieved from BBC News.

EUTELSAT. (2012). Eutelsat Condemns Jamming of Broadcasts From Iran and Renews Appeals for Decisive Action to International Regulators. Paris.

Federal Ministry of Interior Germany. (2011). Cyber Security Strategy for Germany.

Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020, 07 01). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Cambridge University Press*, pp. 364 - 386. doi:10.1017/S2045381720000167

Government of the Russian Federation. (2019). *On the Approval of the Regulations on Conducting Exercises to Ensure the Sustainable, Safe and Comprehensive Functioning of the Internet and the Public Communications Network in the Russian Federation.* Gosudarstvennaya Sistema Pravovoj Informatsii.

Graham, M. (2013, 3 1). Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? The Geographical Journal. doi:10.1111/geoj.12009

Greenberg, A. (2012). *This Machine Kills Secrets.* Dutton.

Greenberg, A. (2016, 8 2). It’s Been 20 Years Since This Man Declared Cyberspace Independence. Retrieved from https://web.archive.org/web/20160211000415/https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/

Hancock, A., & Callas, J. (2022, February 9). *What the Duck? Why an EU Proposal to Require "QWACs" Will Hurt Internet Security*. Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks/2022/02/what-duck-why-eu-proposal-require-qwacs-will-hurt-internet-security

Hare, F. (2006). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? *School of Public Policy, George Mason University*.

Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, pp. 429-434. doi:10.3233/IP-180009

Hubert, B. (2021, May 10). *Dear EU: Please Don't Ruin the Root*. Retrieved from berthub.

Ibarrondo, M. R. (2012). The Censorship-Free Speech Dichotomy in the Internet: an overview.

ICANN. (2022, September 13). *Understanding the Internet’s Domain Name System.* Retrieved from icann.org: https://www.icann.org/en/system/files/files/dns-infographic-13sep22-en.pdf

ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive). (2021, March 19). Retrieved from ICANN.

Ignatius, D. (2021, May 4). *Russias Plot Control Internet is no longer Secret*. Retrieved from The Washington Post.

Internet Governance – Why the Multistakeholder Approach Works. (2016, April 26). Retrieved from Internet Society: https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

ISO. (1994). ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model.

Kleinwächter, W. (2004). BEYOND ICANN VS ITU? How WSIS Tries to Enter the New Territory of Internet Governance. (66 (3–4): 233–51). London: Gazette: The International Journal For Communication Studies. doi:10.1177/0016549204043609

Koch, R. (n.d.). *Cookies, the GDPR, and the ePrivacy Directive.* Retrieved from gdpr.eu: https://gdpr.eu/cookies/

Kolkman, O. (2021, November 5). *NIS2 – Security, Resiliency, and DNS server infrastructure*. Retrieved from Internet Society.

Kolkman, O. (2021, December 17). *NIS2 Inconsistency – a DNS Supply Chain Perspective*. Retrieved from Internet Society.

Komaitis, K. (2022, December 9). *Europe's Risky Plan for the Internet*. Retrieved from directionsblog.eu.

Kostyuk, N., & Zhukov, Y. M. (2019, 02 01). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? (63.2), 317-347. Journal of Conflict Resolution. doi:10.1177/0022002717737138. ISSN 0022-0027. S2CID 44364372

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009, April 1). Cyberpower and National Security. *National Defense University Press*.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. *National Defense University Press*.

Lee, J.-A., & Liu, C.-Y. (2012). Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. *Minn. J.L. Sci. & Tech.*

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). Brief History of the Internet. The Internet Society.

Lessig, L. (2006). *Code 2.0: And Other Laws of Cyberspace.* BASIC BOOKS.

Lloyd, H. A. (1991). Sovereignty: Bodin, Hobbes, Rousseau. *Revue Internationale de Philosophie*(45.179), pp. 353-379.

Marby, G. (2022, March 2). *marby-to-fedorov-02mar22.* Retrieved from icann: https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

Meuller, M. (2010). Networks and States. *MIT Press*, pp. 113-131.

Meuller, M. (2017). Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings. *Digital Policy*, pp. 415-428.

Meuller, M. (2017). Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. *Cambridge: Polity*.

Ministry of Defense UK. (2008). Deputy Secretary of Defense Gordon England.

Moose, J. (2012). Two Stack Layered Model. pp. 80-83.

Nagy, T. B. (1998). Personal Jurisdiction and Cyberspace: Establishing Precedent in a Borderless Era. CommLaw Conspectus 101.

Nanni, R. (2022). The ‘China’ Question in Internet Fragmentation: Evidence From the ‘New IP’ Fragmentation: Evidence From the ‘New IP’. *Centre for Global Cooperation Research*.

Number of internet and social media users worldwide as of July 2022. (2022). Retrieved September 2022, from Statista: https://www.statista.com/statistics/617136/digital-population-worldwide/

Open Network Architecture (ONA). (n.d.). Retrieved from Dialogic: https://www.dialogic.com/glossary/open-network-architecture-ona

Osgood, R. (2004). Net Neutrality and FCC Hack.

Philosophy, S. E. (2020, 6 22). Sovereignty.

Plexida, E. (2022). EU Dimensions of the ‘Splinternet’ Question. *Centre for Global Cooperation Research*.

Protection of Personal Information Act (POPI Act). (n.d.). Retrieved from POPIA: https://popia.co.za/

Raffestin, C. (2012). *Space, territory, and territoriality* (30 ed.). Environment and Planning D: Society and Space. doi:10.1068/d21311

Reimann, M. (2003). Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage. (24.3). Michigan Journal of International Law. Retrieved from https://repository.law.umich.edu/mjil/vol24/iss3/1

Reus-Smit, C. (2013, December). The concept of intervention. *Review of International Studie, Special Issue: Intervention and the Ordering of the Modern World*, pp. 1057-1076.

RIPE NCC Response to the European Commission's Proposed NIS 2 Directive. (2021, March). Retrieved from RIPE NCC.

Ristolainen, M. (2017). Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security within Russia and the West. *Journal of Information Warfare*, pp. 113–131.

Saltaformaggio, B., & Konte, M. (2019, June 28). Understanding the Role of Extended Validation Certificates in Internet Abuse.

Sar, E. V. (2022, January 19). *The EU Wants Its Own DNS Resolver that Can Block 'Unlawful' Traffic*. Retrieved from torrentfreak: https://torrentfreak.com/the-eu-wants-its-own-dns-resolver-that-can-block-unlawful-traffic-220119/

Tambini, D., Leonardi, D., & Marsden, C. T. (2008). Codifying cyberspace : communications self-regulation in the age of internet convergence.

The EU ePrivacy Regulation (ePR). (n.d.). Retrieved from IT Governance.

The International Organization for Standardization, & The International Electrotechnical Commission. (2012). ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity.

The Internet Way of Networking: Defining the critical properties of the Internet. (2020, September 9). Retrieved from Internet Society.

Tiirmaa-Klaar, H. (2016, June 20). *EU International Cyber Policy: promoting a free and secure global cybespace.* Retrieved from Global Forum on Cyber Expertise.

Tropina, T. (2022). Internet Fragmentation: What's at Stake? *Centre for Global Cooperation Research*.

U.S. Department of Defense. (2001). Dictionary of Military and Associated Terms (amended 2007).

U.S. Department of Defense. (2001). Dictionary of Military and Associated Terms (amended 2009).

Verstaeger, M. (2019). *Answers to the European Parliament: Questionnaire to the Commissioner-Designate: Margrethe Vestager, Executive Vice-President-Designate for a Europe Fit for the Digital Age.* Retrieved from European Parliament: https://www.europarl.europa.eu/news/en/hearings2019/commission-hearings-2019/20190910STO60707/margrethe-vestager-denmark

Voge, C., Kolkman, O., & Robachevsky, A. (2021, October 11). *Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021*. Retrieved from Internet Society.

Wallace, N. (2018, March 13). *EU e-privacy proposal risks breaking 'Internet of Things'*. Retrieved from EU Observer.

Wamala, F. (2011, September). ITU National Cybersecurity Strategy Guide. International Telecommunication Union.

Werbach, K. (2002). A Layered Model for Internet Policy. *J. on Telecomm. & High Tech. L 37*.

Werbach, K. (2005). Breaking the Ice: Rethinking Telecommunications Law for the Digital Age. *J. ON T ELECOMM . & HIGH T ECH. L. 59* .

When Regulatory Power and Industrial Ambitions Collide: The “Brussels Effect,” Lead Markets, and the GDPR. (2022). *Privacy Symposium*, pp. 129-151.

Woodward, M. (2021, July 8). *16 Countries with GDPR-like Data Privacy Laws.* Retrieved from Security Scorecard.

Z, N. (2018, April 9). *DNS Market Share Analysis — Identifying the Most Popular DNS providers*. Retrieved from Medium: https://medium.com/@nykolas.z/dns-market-share-analysis-identifying-the-most-popular-dns-providers-80fefb2cfd05