CYBER-SECURITIZATION IN LIGHT OF THE SNOWDEN REVELATIONS: EFFECTS ON INSTITUTIONAL REFORM IN THE US AND EU

Cosmina MOGHIOR
National University of Political Studies and Public Administration
Bucharest/ Romania

Abstract
This article examines the securitization of cybersecurity through a discourse analysis of the Snowden revelations. Using a critical discourse analysis approach, this study explores the language and narratives used by policymakers and other stakeholders in the cybersecurity field to construct and frame cybersecurity threats and responses. The article argues that the securitization of cybersecurity is a complex and multifaceted process that is shaped by a range of social, cultural, and political factors. Through a detailed analysis of official documents, speeches, and media reports, this study reveals the ways in which the Snowden revelations were framed and constructed as a security threat, and how this framing has shaped the development of cybersecurity governance in the US and EU. The article contributes to a more nuanced understanding of the securitization of cybersecurity and highlights the importance of discourse analysis in studying this critical field.

Keywords
Cybersecurity; cybersecurity governance; discourse analysis; Snowden revelations; securitization

1. INTRODUCTION

The rapid digitalization of the modern society has created a complex and vulnerable landscape, where cybersecurity has become a pressing concern. The increasing dependence on digital technologies has led to the emergence of new challenges in cyberspace, with potential threats ranging from information leaks to physical damage. As a result, cybersecurity has become a national priority for many countries, requiring a collaborative effort between the state and the private sector (McNamara 2024). However, this development also facilitated the emergence of powerful private companies leading to the "dilution of the state's role" and "sovereignty gap" in providing security (Kello 2017). This article explores the concept of cybersecurity and its securitization, with a focus on the role of the state in the digital era.

The existing research on cybersecurity has often overlooked the value of discourse analysis in understanding the complex and multifaceted nature of cybersecurity threats and responses. While some studies have employed discourse analysis to examine the language and narratives used by policymakers and other stakeholders in the cybersecurity field, these efforts overlook the power dynamics, social constructions, and cultural norms that shape cybersecurity governance. There is a need for more research that explicitly examines the role of discourse analysis in studying cybersecurity, and that explores the ways in which discourse shapes our understanding of cybersecurity threats, responses, and governance. By filling this research gap, this study aims to highlight the importance of discourse analysis in studying this critical field.

The securitization of cybersecurity is a complex process, influenced by various factors, including the framing of security issues by policymakers and the legitimation of exceptional measures to address these issues. This article examines the securitization of cybersecurity, with a focus on the case of Edward Snowden's revelations about the US National Security Agency's (NSA) surveillance programs. In this article, I aim to respond to the following questions: (1) How do the Snowden revelations illustrate the power of individual actors in mobilizing policy change, and what are the implications of this case for our understanding of cybersecurity governance?; (2) What are the

policy impacts of the Snowden revelations in the US and the European Union?; (3) How does securitization shape our understanding of cybersecurity threats and responses?; (4) How can discourse analysis be used to study the securitization of cybersecurity, and what are the benefits and limitations of this approach?

The article argues that the securitization of cybersecurity is a process that generates wider understanding and acceptance of an issue as a security concern. The discourse analysis of the Snowden case reveals that the securitization of cybersecurity is a complex process, involving various actors, including policymakers, private organizations, and individuals. The article also highlights the importance of understanding the context and the language employed in the securitization discourse, as well as the role of the audience in accepting or rejecting the securitizing actor's utterance. Furthermore, the article examines the policy impact of the Snowden revelations in the US and the European Union, highlighting the changes in surveillance laws and data protection regulations. The article concludes that the securitization of cybersecurity is a complex and ongoing process, requiring a nuanced understanding of the factors that influence it.

2. CYBERSECURITY AND CYBER-SECURITIZATION

Digital companies created an entirely new and complex universe, governed by its own rules and with their specific governance logic based on specific business models. It is a domain that is evolving, while the society is increasingly dependent on the digital sector. Along with the opportunities, we are also witnessing the emergence of new security challenges in cyberspace. The cyber-attacks can affect the targeted entities in a wide range of ways, from information leaks to physical damage. The importance of digital sector is a national priority for most of countries for security, political, and economic reasons. Cybersecurity is a multistakeholder and collaborative endeavour, between the state and the private sector, and a cross-border effort in general (Costea 2023). The

interconnected nature of the digital era makes it is impossible to attain cybersecurity in isolation.

Technically, cyberspace is defined as "a globally networked, computer-sustained, computer accessed and computer-generated, multidimensional, artificial, or 'virtual' reality" (Benedikt 1991, 122). More precise, it is "the publicly accessible global packet switched network of networks that are interconnected through the use of the common network protocol IP" (Malcolm 2008, 1).

The Internet is organized on layers, comprising hardware, software and the transmitters. The users, the physical communication networks and the equipment are subject to the jurisdiction of the states. The layered approach helps with the identification of the sectors where the state may exert sovereign control. The state enjoys authority over the physical layer based on "proximity" principle, linked to territorial physical presence. The state authority is the most limited at the level of *software layers*, consisting of codes and standards (Roguski 2019). Software layers are very abstract and lacking transparency, often avoiding the public regulation making state authority enforcement a difficult task. However, this aspect is gradually changing, with many new pieces of legislation addressing issues of cybercrime, disinformation, or minimum mandatory cybersecurity standards. This section of the Internet infrastructure has also been the subject of public interference for public surveillance purposes in authoritarian states (i.e., Russia and China), but is also on the rise in established democracies (including France).

From a state perspective, cybersecurity definition is data-focused, respectively "state of normality resulting from the implementation of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of electronic information of public or private resources and services in the cyber space" (Parlamentul Romaniei 2023). Other perspectives focus on those efforts, namely the critical infrastructures or individuals (Guinora 2017, 17). The attacks on critical infrastructures "have a crippling impact" on the social and economic stability (Cavelty 2008, 10).

The focus subject in cybersecurity is the state itself as in the classic security but on the protection of the inanimate objects, such as critical infrastructures, with

indirect effects for the citizens who "benefit from an interruption-free performance of vital systems" (Cavelty 2014, 708). The focus is on "the conjoined body of public and private-sector networks" (Der Derian and Finkelstein 2008, 102).

Cybersecurity is now recognized as a significant national security concern, similar to traditional security issues. But what factors contributed to its prominence? Certain exogenous factors may lead to a change in the treat perception of the policymakers and leading to the "securitization" of certain ideas, wherein security issues are formulated from position of power informing future policy choices to address these issues, and legitimation is sought from the audience for these proposals (Farrand and Carrapico 2022) (Kornprobst and Traistaru 2021) (Christou 2018) (Balzacq 2011).

Waever defines the security problems as "developments that threaten the sovereignty or independence of a state in a particularly rapid or dramatic fashion and deprive it of the capacity to manage by itself" (Waever 1995, 72). Having this idea in mind, the policymakers can claim at any time the right to resort to exceptional measures to secure the survival of the state. In other words, "something is a security problem when the elites declare it to be so" (Waever 1995, 73). Waever defined this phenomenon as *securitization* which is a process that generates wider understanding and acceptance of an issue as a security concern. Because of the high importance of discourse in this process, Weaver labelled it as a "a speech act" (Waever 1995, 73).

In the process of cyber-securitization (or any type of securitization for that matter), there are a series of requirements which were met and confirmed the success of securitization process. One is the appropriate position from which the securitizing actor is uttering. The second is the existence of an empowering audience who should decide upon accepting or rejecting that certain utterance. Finally, is employing the appropriate language in the discourse, which is common for both the securitizing actor and the audience.

Myriam Dunn Cavelty defined the securitization of cyberspace as "a combination of linguistic and non-linguistic discursive practices from many different 'communities' of actors" (Cavelty 2013, 108). The nature of the threats from cyberspace and the perception of their criticality can vary across different

communities. The referent objects are being framed in different ways across various communities, mainly because the importance attached to a certain issue is different between cultures and historical heritages. But the diversity of threat perception and the ambiguity of cyberspace are hampering the cyber-securitization underspending.

The threat representation of the *technical domain* is often illustrated through biological analogies. The increasing digital interconnectedness is frequently associated with network vulnerability to virus infection, in a similar way as the human body. Within the *socio-political* cluster, old forms of offences become new by linking them to the prefix "cyber-", which emphasizes the expansion of the environment in which cyber criminals are acting. The actor which is delivering the attacks in cyberspace is also known as "hacker", concept which is loaded with stereotypes. The hacker was initially pictured as a highly skilled, young person (Ross 1990), but it gained negative connotations over time due to the rogue use of these skills. The critical infrastructure is one of the most important referent objects of the *human-machine* cluster. The networks/infrastructures are framed as critical because they are the mechanisms that sustain the functionality and the well-being of the whole society.

Hansen and Nissenbaum have identified three types of security narratives specific to the cyber sector indicating the level of criticality raised by the securitizing actors. The first concept is "hypersecuritization", initially introduced by Barry Buzan in 2004, which indicates "a tendency both to exaggerate threats and to resort to excessive countermeasures" (Buzan 2004, 172). The state is most of the time the referent object for this type of language. Usually, when the elites are employing this narrative are always referring to catastrophic events from the past as a parallel of the present event with the historical one to mobilize and legitimize the (extraordinary) measures for tackling the new threat. But in the case of cybersecurity, there was no catastrophic event to be used as a reference. Hence, the elites are using the "probability" factor or various metaphors to increase the urgency to motivate the need for special measures.

The second grammar of cybersecurity are the "everyday security practices" in which "securitizing actors, including private organizations and businesses,

mobilize ''normal'' individuals' experiences" (Hansen and Nissenbaum 2009, 1165), ultimately building consensus for hypersecuritization. The people and the society are usually the referent objects for this type of language. The securitization of everyday life often refers to dangers including credit card fraud, identity theft, and phishing. The threats in cyberspace are predominantly constituted as threats to the network and hence to society (Hansen and Nissenbaum 2009, 1165). For this type of securitization, the securitizing actors are often employing metaphors form the medical domain, such as viruses, infected computers, protection, contagion etc.

Finally, the third type of discourse arises particularly within the *technical*, expert circles. The audience for this type of discourse requires knowledge to master the field of computer security, which is often unavailable to the broader public (Hansen and Nissenbaum 2009, 1166).

3. CASE SELECTION AND METHODOLOGY

The case of Edward Snowden revelations of the U.S. National Security Agency (NSA) data collection practices is outstanding to illustrate the power of an individual in mobilizing policy change. Furthermore, this case is special for several reasons. Firstly, it underlines the impact of the vulnerabilities in cyberspace on the national security. Secondly, next to the actual information leak which threatened some of US's vital operations, it highlighted the critical importance of cybersecurity protocols in public authorities managing sensitive information. Thirdly, the data extraction was conducted by an "insider" which makes prevention a complex challenge. Lastly, it is important to analyse this case for the motivation behind the act, namely it was described as a social act, not material motivated. Edward Snowden declared that his "sole motive is to inform the public as to that which is done in their name and that which is done against them" (Greenwald, MacAskill and Poitras, Edward Snowden: the whistleblower behind the NSA surveillance revelations 2013).

I will conduct our inquiry at the second level of analysis, namely at the "acts" level. It comprises both discursive and non-discursive markers: the action-type

(the type of language to which the securitizing actors had resorted), heuristic artefacts (markers which aim at mobilizing the audience), devices (practices and tools used in the process of securitization), and the policy generated from the process of securitization (Balzacq 2011, 36). I investigate the manner the Snowden revelations were framed among the US' political elites and other prominent actors, while explaining the reason behind that framing. It is also interesting to look at the level of criticality raised by the securitizing actors after Snowden's act, which might indicate us the level of damage produced by that event. Moreover, I also include an overview of the main policy effects in the European Union in the aftermath of the revelations.

The empirical analysis of this study is based on a critical discourse analysis of official documents, speeches, and media reports related to the Snowden revelations and their impact on cybersecurity governance. The dataset includes a total of 50 documents, including speeches by policymakers, official reports, and media articles, which were collected from publicly available sources. The analysis was conducted using a qualitative content analysis approach.

Using discourse analysis to illustrate the effects of the revelations helps to "map the emergence and the evolution of patterns of representations which are constitutive of a threat image" (Balzacq 2011, 39). Discourses are considered "bodies of texts…that bring new ideas, objects and practices into the world" (Hardy, Phillips and Harley 2004, 20). This idea underlines the aspect that the discourses can take the form of resources (sociocultural instruments) and practices (the actual use of the sociocultural instruments). The discourse analysis shows the transformation of an idea in a security issue (Balzacq 2011, 41).

Among the weakest points of the method of discourse analysis is that it implies the consultation of a vast amount of information and in various forms, from official documents to images. To mitigate this challenge, I focus my analysis primarily on the members of the US Intelligence Community (IC) and secondarily on other important actors, such as the US President and several key-spokespersons. Therefore, I find insightful to look at discourses from NSA, Department of Defense (DoD), the Office of the Director of National Intelligence (DNI) and many other intelligence agencies, but we will also consult the US Government website. The period I analyse is between June 2013 until 2017,

when the Members of Congress decided then to pass the FISA Amendments Reauthorization Act on the continuation of the NSA surveillance programs. The section of the effects on the European Union policy has an open-ended time interval, since this event is still felt today, more than 10 years later.
The interpretation of data is by examining the internal coherence (intratextuality) of the statements (identifying their objectives, heuristic artefacts and the generated interaction) and analysing by analysing the relationship between the patterns of threat representation in different texts (intertextuality) (Balzacq 2011, 43).

4. THE CYBER-SECURITIZATION OF THE SNOWDEN REVELATIONS

4.1 The context

On 20th May 2013 an NSA contractor, left the US for Hong Kong carrying four laptop computers loaded with secret information extracted from NSA's database. He followed by publicly disclosing some of the American Intelligence Community (IC)'s most kept secrets about surveillance operations in the U.S. and abroad. He shared the information with the journalists Glenn Greenwald and Ewen MacAskill from the publication The Guardian and the documentary filmmaker Laura Poitras (Gidda 2013).
The first revelation published in The Guardian reported the NSA's domestic email and telephone surveillance from Verizon. The journalist Glenn Greenwald elaborated on the type of data that NSA was collecting, stressing the fact that NSA "has transformed from an agency exclusively devoted to foreign intelligence gathering, into one that focuses increasingly on domestic communications" (Greenwald 2013).
A few days after the disclosures, the identity of the source have been revealed. His name is Edward Snowden, a 29-year-old, former IT specialist for Central Intelligence Agency (CIA) and a current contractor for Booz Allen Hamilton, at the time of revelation. After working for several years within various

intelligence agencies, Snowden decided to make public the IC's surveillance programs, which in his perspective are "abuses". He stressed that those practices have "to be determined by the public not by someone who is simply hired by the government" (Greenwald, MacAskill and Poitras 2013).

This disclosure revealed the NSA's powers conveyed by programs such as PRISM (in which the agency has direct access to some of the biggest server firms, including Microsoft, Yahoo, Google, Facebook, Apple and many other), Boundless Informant (a mapping and auditing tool for global surveillance data) and XKeyscore (a database filled with the online activities of millions of people) (Greenwald and MacAskill 2013). These are programs created in the aftermath of 9/11, as a measure of ensuring national security through public surveillance using digital means.

The journalists highlight the fact that once the audience have accepted the utterance, the issues can be moved to the level of extraordinary countermeasures and can even be developed into secrecy if is inserted in a "package legitimization" (Greenwald 2013) which does not require approval from the public. This phenomenon also underlines the fact that the securitization can re-define the *status quo,* making it almost impossible or at least difficult for the public to question or contest the measures taken by the state. One of the main reasons is because the activities, measures, or decisions are taken under major secrecy.

4.2. Initial reaction of the US elites

Snowden's revelations have created reactions across the board among the US political elites, who called him names from "social activist" to "traitor". The strongest reactions came from the Speaker of the United States House of Representatives John Boehner, calling Snowden a "traitor" perceiving the disclosures have "damaged our ability to keep Americans safe here and abroad" (French 2014).

A mid-range reaction to the disclosures have been delivered by the President Barack Obama, who called Snowden a "hacker" (Obama, Remarks by President

Obama and President Sall of the Republic of Senegal at Joint Press Conference 2013), reducing the level of criticality raised by the other political actors. Obama and his spokespersons insisted on reassuring the public that even though the disclosures "caused harm to…national security and interests" it was not the case for taking extraordinary measures. This was just another case which ought to be "routinely dealt between law enforcement officials in various countries" (Obama, Remarks by President Obama and President Sall of the Republic of Senegal at Joint Press Conference 2013).

The Obama administration tried to avoid promoting the event by raising the criticality of the impact. Firstly, it created a series of tensions between US and the two countries where Snowden found refuge, namely China and Russia. Secondly, President Obama stressed that "the damage was done with respect to the initial leaks" (Obama, Remarks by President Obama and President Sall of the Republic of Senegal at Joint Press Conference 2013), reason why he did not intend to "start doing wheeling and dealing and trading" for prosecuting a felon (Obama, Remarks by President Obama and President Sall of the Republic of Senegal at Joint Press Conference 2013). Obama specifically condemned Snowden's method of distribution of the material extracted from NSA, pointing to the existing whistleblowing channels and procedures without harming the national security and breaking the law (Obama, Interview of the President by Jay Leno, The Tonight Show 2013).

There was also a category of political elites who welcomed the disclosures. Senator Bernie Sanders stated that, although he broke the law for which he should be punished, Snowden "played a very important role in educating the American people" (Thielman 2015). The US attorney general Eric Holder said that even though the disclosures have been made in an inappropriate and illegal way, Snowden had "performed a public service by raising [a national] debate" (Holpuch 2016).

The US House of Representatives' Permanent Select Committee on Intelligence (HPSCI) drafted a review of the case. The Committee specified that they could not find any "evidence that Snowden attempted to communicate concerns about the legality or morality of intelligence activities to any officials" (House Permanent Select Committee on Intelligence 2016). The HPSCI review

concluded that Snowden is not considered a whistle-blower under the current law because he did not file a complaint with the DoD or Department of Defense Inspector General (IC IG) office to raise concerns about the unlawful practices. In exchange, he disclosed classified information to the press (House Permanent Select Committee on Intelligence 2016).

By mid-June, the United States District Court for the Eastern District of Virginia charged Snowden with "violating the Espionage Act and stealing government property for disclosing classified information to The Guardian and The Washington Post" (Shane 2013). The Court decided that Snowden have brought three offenses: "theft of government property; unauthorized communication of national defense information; and wilful communication of classified communications intelligence information to an unauthorized person" (United States of America v. Edward J. Snowden 2013, 1).

While media kept on framing Snowden as a whistle-blower, the White House's Press Secretary Jay Carney underlined that Snowden has been charged for "leaking classified information. He is not a dissident. He's not a whistle-blower. He's been charged with a crime" (Carney, Press Briefing by Press Secretary Jay Carney, 8/1/2013 2013). In the aftermath of the disclosures, Snowden called for the whistle-blower protection (Ackerman and MacAskill 2016), which was rejected mainly because he did not follow the established procedure for signalling the abuses (Earnest 2016).

The former Director of National Intelligence, James Clapper stated in a conference at the University of Georgia that as a consequence of the disclosures "our nation is going to be less safe and our people less secure" (Clapper 2014). A few years later he stated in an interview that the disclosures extended beyond the domestic surveillance, exposing, and compromising vital intelligence operations home and abroad. He stressed that Snowden "compromised a lot of our capabilities and if you're a taxpayer you're going to be paying, we all are, to recover from the damage that he caused" (O'Hehir 2018). Although Snowden motivated his act for informing the public, the information released was considered "extremely damaging to our national security and gives our terrorist enemies a playbook for our activities designed to thwart them" (Carney 2013).

4.3. The securitization language employed by the US elites

The disclosure of NSA's secret information is a case which was predominantly framed in terms of the Espionage Act violation and information theft and disclosure to unauthorized people, rather than in cybersecurity terms. Snowden's motivation was redemptive, aiming to launch a public debate of what he perceived to be an "abuse" in the Intelligence Community's operations (Greenwald, MacAskill and Poitras 2013). The securitization discourse was predominantly oriented on the NSA's networks vulnerabilities to insider threats. This aspect was also highlighted by President Obama stating that the disclosures showed NSA's most "significant vulnerabilities" (Obama 2013).

The revelations had a considerable impact on the American society, both at the high level among elites and the society. The review of the U.S. House of Representatives' Permanent Select Committee on Intelligence published in 2016 presents the unauthorized disclosures of the former NSA contractor Edward Snowden and the impact of these disclosures on the IC and the American society. The Committee reviewed Snowden's behaviour in his process of revelling the secret information, from actions to motivations. The Committee analysed a series of documents form the IC and conducted several interviews with key-people who had knowledge about Snowden's background and actions in connection to his act. The review includes information about Snowden's background from his early life to the moment of the revelations. Furthermore, the Committee analysed Snowden's legal status in terms of procedures followed by the actor in the revelations (House Permanent Select Committee on Intelligence 2016).

The HPSCI used extensively the technification grammar in their review, precisely through focusing on framing the case as an issue of IC's critical vulnerability to unexpected and inevitable dangers arising from within the community. In their review, the Committee discovered that NSA was not aware of its vulnerabilities with respect to Snowden's actions, because his "work responsibilities involved transferring large amounts of data" (House Permanent Select Committee on Intelligence 2016, 13). The vulnerability aspect is further articulated when the Committee described the methods used by the actor to

extract the information from NSA's database, "none of which required advanced computer skills" (House Permanent Select Committee on Intelligence 2016, 10). Initially, the actor used "blunt tools" or "scraping" tools called "wget" and DownThemAll! to extract "all" the information form NSA's classified networks. Afterwards, he used his administrator privileges access offered by his job to access NSA's employees' personal network devices where he collected everything he could find (House Permanent Select Committee on Intelligence 2016, 10-11).

The Committee stressed that although these types of vulnerabilities can be reduced through simple changes such as "detecting the malicious use of scraping tools…physically disabling removable media from the workstation… and implementing two-person controls to transfer data" (House Permanent Select Committee on Intelligence 2016, 29) it is still impossible to eliminate any potential similar cases. In the light of such vulnerabilities, the Committee remained concerned that the IC "have not done enough to reduce the chances of future insider threats like Snowden" (House Permanent Select Committee on Intelligence 2016, 29). Furthermore, the vulnerability aspect also arises from the period of extraction span, which extends from roughly July 12, 2012, after a conflict with some of NSA's managers, until his last day inside the agency, May, 2013. When he obtained a new position of contractor in March 2013 at Booz Allen Hamilton, he had even more access to secret information, opportunity which he took advantage for removing more documents (House Permanent Select Committee on Intelligence 2016, 15).

There are a series of technification markers in the HPSCI's cyber-securitization discourse. Firstly, it refers to the aspect that Snowden's position within the IC implied access to highly sensitive information and that the agency could not detect his suspicious behaviour in a timely manner. The Snowden's disclosures highlighted one of agency's vulnerabilities, which is almost impossible to eliminate entirely. Secondly, it talks about the rudimentary methods used by Snowden to download a massive amount of information. This point re-emphasizes the fact that one does not necessarily require sophisticated instruments to harm US and its interests. This situation comes in contradiction with the language employed in the cybersecurity strategies describing threats

coming from sophisticated actors employing complex methods and calling for extraordinary measures (Executive Office of the President of the US 2003, 3, 6, 19, 24, 40) (Executive Office of the President of the US 2011, 8, 13, 20). Thirdly, the vulnerability is captured in the time span in which Snowden download the files, which is almost one year. During such a long time, the agency was not aware of his actions or objectives.

The hyper securitization grammar markers are also present in the document, but not as often as the technification ones. The Commission specified that "the vast majority of the documents Snowden removed were unrelated to electronic surveillance or any issues associated with privacy and civil liberties" (House Permanent Select Committee on Intelligence 2016, 22). Furthermore, from a limited damage assessment of the disclosed documents from the Tier One (referring to aspects related to "rogue states threatening regional stability or major strategic powers and a few transnational issues such as [weapon] proliferation" (Deutch 1995)) the Committee indicated that "Snowden's disclosures caused massive damage to national security" (House Permanent Select Committee on Intelligence 2016, 24).

The Committee accentuated that Snowden's intents were not as pure as it was pictured. Instead of collecting information suited to his "mission", he downloaded "all" the sensitive information (indiscriminately), including information related to vital operations domestically and abroad. The Committee delegitimized Snowden's intents by stressing that only a small portion of the documents were related to surveillance and other privacy and liberties aspects. Lastly, the Committee employed the hyper securitization expression "massive damage to national security" which enhances the criticality framed by the Committee.

5. THE POLICY IMPACT OF THE REVELATIONS IN THE US AND THE EU

5.1. Policy changes in the U.S.

The US House Permanent Select Committee on Intelligence drafted the review for the Members of Congress and for American people ("where possible") to explain how "most massive and most damaging theft of intelligence information in our history by Edward Snowden" occurred (Clapper 2014, 6). Following this report, the Members of Congress decided the to pass the FISA Amendments Reauthorization Act of 2017, regarding the continuation of the NSA surveillance programs. However, it comes with a reassuring for the American population with the section 702, which "provides robust privacy protections for American citizens, and most importantly prohibits the Government from using it to target Americans and persons located in the United States" (Trump 2018).

Snowden himself was an alternative securitizing actor, by signalling the irregularities within the American IC. His act has been perceived as a resistance move against the IC's practices, which is a form of "countering elite utterances of security by seeking out dissenting or marginalized securitizing moves or counter-securitization claims" (Charrett 2009, 25-26). Through his utterance, he highlighted the perceived abuses performed by the state through the surveillance programs. What Snowden lacked for a successful securitization is the appropriate position of authority. He did start a public debate, which was one of his aims. Unfortunately, his main aim was to influence the IC's unlawful practices. The surveillance programs which he spoke against were part of the Foreign Intelligence Surveillance Act (FISA), which was renewed in 2018. It is a document which allows the continuation of the NSA surveillance programs. His act did lead to considerable changes within the IC, such as reforms to increase the security and prevent any other the potential leaks and accelerated the creation of the IC IT Enterprise. However, his aim was to encourage the IC to allow more transparency in their practices and to reduce the privacy breaches created through its surveillance programs. As most of the IC's surveillance

practices are classified, we cannot verify if or to what extent the surveillance programs developed since the disclosures.

Although the surveillance practices were agreed to continue through the adoption of the FISA Amendments Reauthorization Act in 2017, Snowden's utterance triggered a series of changes within the American and international society, at all levels. What followed the disclosures is often called "The Snowden effect" (Bryant 2013). It was especially felt within the US diplomacy which was seriously affected by the lack of trust from various foreign officials, such as Brazilian President Dilma Rousseff, German Chancellor Angela Merkel, French President Francois Hollande and 35 other world leaders who have been monitored by NSA (Bryant 2013). Moreover, German Chancellor Angela Merkel stated that "[t]rust will now have to be rebuilt" (Bryant 2013).

The Snowden disclosures have triggered major changes with respect to surveillance. Unthinkable before the leaks, the USA Freedom Act that places restrictions and oversight on the NSA's surveillance powers have been adopted by both houses of Congress (Cohn and Reitman 2015). The leaks also launched a series of cases which are challenging NSA's surveillance operations' legal and constitutional grounds: First Unitarian v. NSA; Jewel v. NSA; Hepting v. AT&T (Reitman 2016). Moreover, it clarified the "broken relationship between the intelligence community and the public" (Reitman 2016) on the matter of surveillance.

The revelations have unveiled the NSA's data collection using some of the major companies, such as Apple, Google, Facebook, and Yahoo. The tech companies do not want to be associated with the NSA surveillance operations, as it harms their businesses. Most of the companies did not comment on the disclosures, except for Microsoft and Yahoo. Following the disclosures, Yahoo reported that they fought against NSA's demands before joining PRISM operations requesting to unseal the documents on that confrontation. They invoked the Fourth Amendment, which states the illegality of the unreasonable searches and seizures, but the Court concluded that it was not the case, hence, the company had to hand out the information (Musil 2013). Brad Smith, Microsoft's chief legal officer stated that the company have learned "the importance of standing up for privacy rights. To some degree, I think our whole industry needed to react to

what we learned in the wake of the Snowden disclosures. We learned things of which we were not aware. And we came away from that with a renewed determination to protect privacy and I think what we at Microsoft were able to do was harness all the learning we had gained through all the legal issues around the world, and really use that to be more proactive" (Lillington 2016).

5.2. Policy changes in the European Union

The Edward Snowden revelations in 2013 had significant policy effects in the European Union, particularly in areas of data protection, privacy rights, and transatlantic relations. Moreover, the revelations showed that "democracies employ similar surveillance tactics as authoritarian states" (Codreanu 2024). Starting with the data protection policy, studies show that the salience of Internet privacy issues in the media have increased substantially, opening the avenue for pro-privacy advocates to promote more stringent rules in the area (Antoine 2022). In addition to politicization in the media of the issues of data protection, the revelations contributed significantly to the EU regulation development, opening the avenue for public debate to impact the decision-making (Bennett and Raab 2018). Andrus Ansip, Commission Vice-President for the Digital Single Market stated that "The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information" (European Comission 2015).

The Snowden revelation mobilized a broader debate around digital sovereignty in the EU. This concept revolves around the idea that the Member States should maintain control over the digital infrastructures, reducing dependency on critical technologies from third countries, and ensuring that the technologies and the data processing practices align with the EU norms and values. Snowden accelerated an already existing debate around data protection and a push for data localization on EU territory. Several data-related policy initiatives emerged in the EU, notably the GAIA-X (Gaia-X n.d.), launched by France and Germany in 2019, with the aim of creating a secure and transparent European cloud

infrastructure, while promoting the emergence of European champions capable of ensuring technological independence and sovereignty with respect to data usage and storage (Pannier 2021). However, the initiative was strongly criticised for including American and Chinese cloud companies among the members (Mélin 2021). This membership structure even pushed for the self-exclusion of a leading European cloud computing company (Speed 2021).

When it comes to data protection, the EU has a long history, starting with the Data Protection Directive (DPD) in 1995 which met strong resistance from the public at the time. Several years later when the discussions started on the General Data Protection Regulation GDPR) around the beginning of 2010s, the opinions from various stakeholders only grew more critical towards tougher rules on the issue. From the private sector, lobby, and Member States raised their disagreement with the level of prescriptiveness and the obligations proposed in the new draft legislation. The resistance was so fierce that the Commissioner Viviane Reding argued that she would strive to maintain in the new regulation at least the "current level of protection as laid down in the 1995 Directive" (Reding 2013).

The Snowden's revelations provided a complete change of context for the work on this file in the EU making it very clear that the "data protection reform is Europe's answer" (European Commission 2013). It created the right policy window to strengthen the GDPR by changing completely the narrative from a general debate on Internet privacy to a fundamental discussion on the "self-determination and dignity" (Schuster 2013) of the Europeans and their protection from "unwanted and abusive American surveillance" (General Data Protection Regulation 2016).

The Snowden revelations also raised concerns about the safety of personal data being transferred from the EU to the U.S., especially given the extensive surveillance practices revealed. This event led to a decision by the European Court of Justice invalidating the Safe Harbor (Court of Justice of the European Union 2015), a mechanism adopted in 2000 to allow U.S. companies to meet the protection standards required by the DPD. The decision followed a complaint brought by the privacy activist Maximillian Schrems, concerning Facebook's data transfer policy from EU to the U.S. (Financial Times 2015).

The invalidation of the Safe Harbor opened the debate for a new and safer data transfer agreement between EU and the U.S. following the disclosure of the American surveillance activities. Despite the requests of the European data protection officials and Members of the European Parliament to suspend Safe Harbor, the European Commission rejected on the arguments that it would have adverse effects on the EU business interests and the transatlantic economy (Weiss and Archick 2015). Therefore, a new agreement was negotiated, known as Privacy Shield, as a new mechanism for the EU-U.S. data transfer in 2016 (Monteleone and Puccio 2018).

However, amidst the adoption of the U.S. Cloud Act (US Cloud Act 2019) providing the Government the power to request data stored by major cloud providers, even if they are located outside the U.S. territory, a new a second Schrems case was raised with CJUE. The privacy activist raised that the personal data transferred by Facebook to its U.S. headquarters would make it available to U.S. intelligence agencies. CJUE invalidated the EU-U.S. Privacy Shield Framework, highlighting concerns over the American surveillance practices and inadequate protections for EU citizens' personal data under U.S. law (Court of Justice of the European Union 2020). In 2022, the EU and U.S. announced plans to negotiate a new data transfer agreement called the EU-U.S. Data Privacy Framework (European Commission 2023) which was finalized in July 2023. This new framework aims to address the concerns raised in the Schrems II case, notably the access of data by U.S. intelligence authorities and a stronger obligation for companies processing data transferred from the EU.

The e-Evidence Act also emerged in the aftermath of the Snowden revelations. The Act provides for a framework for cross-border and international cooperation between the law enforcement authorities. With the digitalization development and the lack of borders in service provision for platform companies, the investigators required access to electronic evidence that is often located with foreign service providers (e-Evidence Act 2023). The Snowden revelations highlighted the "need for a reliable framework on both sides". Furthermore, the European Parliament put more emphasis on "the necessary protections for the rights of all users" (Bauer-Bulst 2024) when it comes to the processing of personal data.

More generally, the Snowden revelations had profound political implications in the EU, contributing to a redefinition of the external policy towards the U.S. It raised questions about trust in the transatlantic relationship, including when it was revealed that the NSA was monitoring the communications of European leaders, such as German Chancellor Angela Merkel (Reuters 2021). This event sparked diplomatic tensions. Despite the scepticism regarding U.S. surveillance practices, the transatlantic relationship overcame this pressure with the re-emergence of common threat from Russia following the annexation of Crimea (Howorth 2018).

6. CONCLUSIONS

In conclusion, this article has demonstrated the value of discourse analysis in understanding the securitization of cybersecurity. This was done through the analysis of the impact of the Snowden revelations on cybersecurity governance and policy. The case illustrates the power of individual actors in mobilizing policy change, as Snowden's disclosures led to a major shift in the global debate on surveillance and privacy. The implications of this case for our understanding of data protection are profound, highlighting the need for greater transparency and accountability in the development and implementation of law enforcement practices.

The policy impacts of the Snowden revelations in the US and the European Union have been substantial, with significant changes to surveillance laws and data protection regulations. In the US, the USA Freedom Act was passed, placing restrictions on the NSA's surveillance powers, while in the EU, the General Data Protection Regulation (GDPR) was implemented, providing stronger protections for personal data. These changes reflect a growing recognition of the need to balance national security concerns with individual privacy and civil liberties.

The securitization of cybersecurity has been shown to shape our understanding of cybersecurity threats and responses, with the Snowden revelations highlighting the need for a more nuanced approach to cybersecurity

governance. The study has demonstrated how securitization can be used to frame cybersecurity threats in a way that justifies extraordinary measures, but also how this framing can be contested and challenged.

Finally, this study has demonstrated the value of discourse analysis in studying the securitization of cybersecurity. By examining the language and narratives used by policymakers and other stakeholders, we can gain a deeper understanding of the complex and multifaceted nature of cybersecurity threats and responses. The benefits of this approach include the ability to identify and challenge dominant discourses, and to promote a more nuanced and critical understanding of cybersecurity governance. However, the limitations of this approach include the need for careful consideration of the context and power dynamics in which discourses are produced and consumed.

Future avenues for research could include exploring the role of other actors, such as non-state actors and civil society organizations, in shaping the securitization of cybersecurity. Additionally, further research could examine the impact of emerging technologies, such as artificial intelligence and the Internet of Things, on the securitization of cybersecurity. Furthermore, a comparative analysis of the securitization of cybersecurity across different regions and countries could provide valuable insights into the ways in which different cultural, social, and political contexts shape cybersecurity governance.

REFERENCES

- Ackerman, Spencer & MacAskill, Ewen. 2016. "Snowden calls for whistleblower shield after claims by new Pentagon source." The Guardian, May 22, 2016. Retrieved June 20, 2024. https://www.theguardian.com/us-news/2016/may/22/snowden-whistleblower-protections-john-crane.
- Antoine, Elise. 2022. "The politicisation of internet privacy regulation." *European Journal of Political Research,* 62(2): 530-550. https://doi.org/10.1111/1475-6765.12562.
- Balzacq, Thierry. 2011. *Securitization Threory. How security problems emerge and dissolve.* London and New York: Routledge.

- Bauer-Bulst, Cathrin. 2024. "Interview – Cathrin Bauer-Bulst, European Commission." *Journal of Cyber Policy*, 9(1): 63-93. https://doi.org/10.1080/23738871.2024.2336185.
- Benedikt, Michael. 1991. "Cyberspace: Some Proposals". In: M. Benedikt, *Cyberspace: First Steps*, 119-124. Cambridge, Massachusetts, London: The MIT Press.
- Bennett, Colin J. & Raab, Charles D. 2018. "Revisiting the governance of privacy: Contemporary policy instruments in global perspective." *Regulation & Governance*, 14(3): 447-464. https://doi.org/10.1111/rego.12222.
- Bryant, Nick. 2013. "The Snowden effect on US diplomacy." BBC News, October 24, 2013. Retrieved June 19, 2024. https://www.bbc.com/news/world-us-canada-24664045.
- Buzan, Barry. 2004. *The United States and the great powers: world politics in the twenty-first century.* Cambridge: Polity Press.
- Carney, Jay. 2013. "Daily Briefing by Press Secretary Jay Carney." The White House. President Barack Obama, June 24, 2013. Retrieved June 19, 2024. https://obamawhitehouse.archives.gov/the-pressoffice/2013/06/24/daily-briefing-press-secretary-jay-carney-6242013.
- Carney, Jay. 2013. "Press Briefing by Press Secretary Jay Carney." The White House. President Barack Obama, August 1, 2013. Retrieved June 19, 2024. https://obamawhitehouse.archives.gov/the-press-office/2013/08/01/press-briefing-press-secretary-jay-carney-812013.
- Cavelty, Myriam Dunn. 2008. *Cyber-Security and Threat Politics. US efforts to secure the information age.* New York: Routledge.
- Cavelty, Myriam Dunn. 2013. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse". *International Studies Review*, 15: 105–122. https://doi.org/10.1111/misr.12023.
- Cavelty, Myriam Dunn. 2014. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics*, 20: 701–715.
- Charrett, Catherine. 2009. "A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security." *International Catalan Institute for Peace*, 1-48.
- Christou, George. 2018. "The collective securitisation of cyberspace in the European Union." *West European Politics*, 42(2): 278-301. https://doi.org/10.1080/01402382.2018.1510195.

- Clapper, James. 2014. "Lecture at the University of Georgia", April 14, 2014.
- Clapper, James. 2014. *Testimony on Current and Future Worldwide Threats to the National Security of the United States.* Washington DC: US Senate on Armed Services. https://www.govinfo.gov/content/pkg/CHRG-113shrg93412/html/CHRG-113shrg93412.htm.
- Cohn, Cindy & Reitman, Rainey. 2015. "USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here." Electronic Frontier Foundation, June 2, 2015. Retrieved June 19, 2024. https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here.
- Court of Justice of the European Union. 2015. "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid.", Press release no. 117/15, October 6, 2015. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.
- Court of Justice of the European Union. 2020. The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield.", Press release no. 91/20, July 16, 2020. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.
- Der Derian, James, & Finkelstein, Arthur. J. 2008. "Critical infrastructures and network pathologies: The semiotics and biopolitics of heteropolarity." In: M. D. Cavelty, & K. S. Kristensen (eds.), *The politics of securing the homeland: critical infrastructure, risk and securitisation*, 84-405. London: Routledge.
- Deutch, John. 1995. "Speech: The Future of US Intelligence -- Charting a Course for Change." Central Intelligence Agency, November 7, 1995. Retrieved July 04, 2024. https://irp.fas.org/cia/product/dci_speech_91295.html.
- Earnest, Josh. 2016. "Press Briefing by Press Secretary Josh Earnest, 5/31/2016." The White House. President Barack Obama. Retrieved June 19th, 2024. https://obamawhitehouse.archives.gov/the-press-office/2016/05/31/press-briefing-press-secretary-josh-earnest-5312016.
- European Comission. 2015. "Agreement on Commission's EU data protection reform will boost Digital Single Market." Press release, December 15, 2015. Retrieved June 19, 2024. http://europa.eu/rapid/press-release_IP-15-6321_en.htm

- European Commission. 2013. "Memo: Informal Justice Council in Vilnius.", July 19, 2013. https://ec.europa.eu/commission/presscorner/detail/en/memo_13_710.
- European Comission. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
- European Commission. 2023. *Commission Implementing Decision of 10.07.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.* Official Journal of the European Union. https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng.
- European Comission. 2023. *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. (e-Evidence Act)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng.
- Executive Office of the President of the US. 2003. *The National Strategy to Secure Cyberspace.* Washington: The White House. https://georgewbush-whitehouse.archives.gov/pcipb/.
- Executive Office of the President of the US. 2011. *The International Strategy for Cyberspace.* Washington: The White House. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
- Farrand, Benjamin, & Carrapico, Hellen. 2022. "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity." *European Security*, 31(3): 435-453. https://doi.org/10.1080/09662839.2022.2102896.
- Financial Times. 2015. "Max Schrems: the student who scuppered the EU data." Financial Times, October 6, 2015. https://www.ft.com/content/874a6bd4-6c36-11e5-aca9-d87542bf8673.
- Gidda, Miren. 2013. "Edward Snowden and the NSA files – timeline". The Guardian, August 21, 2013. Retrieved June 19, 2024. https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

- Greenwald, Glen. 2013. "NSA collecting phone records of millions of Verizon customers daily." The Guardian, June 6, 2013. Retrieved June 19, 2024. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
- Greenwald, Glen, & MacAskill, Ewen. 2013. "NSA Prism program taps in to user data of Apple, Google and others." The Guardian, June 7, 2013. Retrieved June 19, 2024. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
- Greenwald, Glen, MacAskill, Ewen, & Poitras, Laura. 2013. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." The Guardian, June 11, 2013. Retrieved June 10, 2024. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
- Guinora, Amos N. 2017. *Cybersecurity. Geopolitics, law, and policy*. London and New York: Routledge.
- Halub, Przemek. 2023. "About Gaia-X - it all starts with data." Gaia-X.eu, December 4, 2023. Retrieved September 2024. https://gaia-x.eu/what-is-gaia-x/about-gaia-x/.
- Hansen, Lele, & Nissenbaum, Hellen. 2009. "Digital Disaster, Cyber Security, and the Copenhagen school." *International Studies Quarterly*, 53(4): 1155–1175.
- Hardy, Cynthia, Phillips, Nelson, & Harley, Bill. 2004. "Discourse analysis and content analysis: Two solitudes?" *Qualitative Methods,* 2(1): 19-22.
- House Permanent Select Committee on Intelligence. 2016. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden.* Washington: US House of Representatives. https://www.congress.gov/congressional-report/114th-congress/house-report/891/1.
- Howorth, Jolyon. 2018. "Strategic autonomy and EU-NATO cooperation: threat or opportunity for transatlantic defence relations?" *Journal of European Integration*, 40(5): 523-537. https://doi.org/10.1080/07036337.2018.1512268.
- Kello, Lucas. 2017. *The Virtual weapon and international order.* New Haven: Yale University Press.
- Kornprobst, Michael, & Traistaru, Corina-Ioana. 2021. "Discourse, Language, and Grand Strategy." In: T. Balzacq, & R. Krebs, *The Oxford Handbook of Grand Strategy*, 173-189. Oxford: Oxford University Press.

- Lillington, Karlin. 2016. "Microsoft's Brad Smith talks privacy, Snowden and international law." The Irish Times, October 4 2016. Retrieved June 19, 2024. https://www.irishtimes.com/business/technology/microsoft-s-brad-smith-talks-privacy-snowden-and-international-law-1.2816460.
- Malcolm, Jeremy. 2008. *Multi-Stakeholder Governance and the Internet Governance Forum*. Perth: Terminus Press.
  McNamara, Kathleen R. 2024. "Transforming Europe? The EU's industrial policy and geopolitical turn." *Journal of European Public Policy*, 31(9): 2371-2396. https://doi.org/10.1080/13501763.2023.2230247
- Mélin, Joëlle. 2021. "Question to the Commission: GAIA-X: contradictions in the Treaties challenge the EU's independence." European Parliament. https://www.europarl.europa.eu/doceo/document/E-9-2021-005332_EN.html.
- Monteleone, Shara, & Puccio, Laura. 2018. *The Privacy Shield: Update on the state of play of the EU-US data transfer rules. In-Depths Analysis*. European Parliament. Directorate-General for Parliamentary Research Service. July 26, 2018. https://data.europa.eu/doi/10.2861/675548.
- Musil, Steven. 2013. "Yahoo reportedly fought court order before joining PRISM." Cnet.com, June 13, 2013. Retrieved June 19, 2024. https://www.cnet.com/news/yahoo-reportedly-fought-court-order-before-joining-prism/.
- Obama, Barack. 2013. "Interview of the President by Jay Leno. The Tonight Show." The White House. President Barack Obama, August 7, 2013. Retrieved June 20, 2024. https://obamawhitehouse.archives.gov/the-press-office/2013/08/07/interview-president-jay-leno-tonight-show.
- O'Hehir, A. 2018. "James Clapper on Donald Trump, Edward Snowden, torture and "the knowability of truth"." Salon, May 26, 2018. Retrieved September 25, 2024. https://www.salon.com/2018/05/26/james-clapper-on-donald-trump-edward-snowden-torture-and-the-knowability-of-truth.
- Pannier, Alice. 2021. "The Changing Landscape of European Cloud Computing Gaia-X, the French National Strategy, and EU Plans." *Briefings de l'Ifri,* July 22, 2021. Paris: French Institute of International Relations**.** https://www.ifri.org/en/memos/changing-landscape-european-cloud-computing-gaia-x-french-national-strategy-and-eu-plans.
- Romanian Parliament. 2023. *Law no. 58 on Romania's cyber secutrity and defense, as well as for the amendment and completion of certain normative acts (Legea nr. 58 privind securitatea şi apărarea cibernetică a României, precum şi*

pentru modificarea şi completarea unor acte normative). 14 March 2003. Monitorul Oficial.

- Reding, Viviane. 2013. "Vice-President Reding's intervention during Justice Council Press Conference." European Commission, June 6, 2013. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_13_514
- Reitman, Rainey. 2016. "3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance." Electronic Frontier Foundation, June 5, 2016. Retrieved June 19, 2024. https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.
- Reuters. 2021. "U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR." Reuters, May 31, 2021. https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/.
- Ross, Andrew. 1990. "Hacking Away at the Counterculture." *Postmodern Culture*, vol. 1(1), September. Princeton University. Retrieved May 19, 2024. http://pmc.iath.virginia.edu/text-only/issue.990/ross-1.990.
- Schuster, Simon. 2013. "E.U. Pushes for Stricter Data Protection After Snowden's NSA Revelations." TIME, October 21, 2013. https://world.time.com/2013/10/21/e-u-pushes-for-stricter-data-protection-after-snowden-nsa-revelations/.
- Shane, Scott. 2013. "Ex-Contractor is Charged in Leaks on N.S.A. Surveillance." New York Times, June 22, 2013. Retrieved June 19, 2024. https://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html.
- Speed, Richard. 2021. "EU digital sovereignty project Gaia-X opens its summit with the departure of Scaleway." The Register, November 19, 2021. https://www.theregister.com/2021/11/19/scaleway_gaia_x/.
- Thielman, Sam. 2015. "Hillary Clinton and Bernie Sanders call for Edward Snowden to face trial." The Guardian, October 14, 2015. Retrieved June 10, 2024. https://www.theguardian.com/us-news/2015/oct/13/clinton-sanders-snowden-nsa-democratic-debate.
- Trump, Donals. 2018. "Statement by the President on FISA Amendments Reauthorization Act of 2017." The White House, January 19, 2018. Retrieved June 19, 2024. https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-fisa-amendments-reauthorization-act-2017/.

- Waever, Ole. 1995. "Securitization and Desecuritization". In: R. Lipschutz, *On Security*, 46-86. New York: Columbia University Press.
- Weiss, Martin & Archick, Kristin. 2015. "The EU-U.S. Safe Harbor Agreement on Personal Data Privacy: In Brief." *Congressional Research Service*, October 29, 2015. https://digital.library.unt.edu/ark:/67531/metadc795682/.
- ***. 2013. United States of America v. Edward J. Snowden, 1:13 CR 265 (CMH) (United States District Court for the Eastern District of Virginia 06 14, 2013).
- ***. 2013. "Remarks by President Obama and President Sall of the Republic of Senegal at Joint Press Conference." The White House. President Barack Obama, June 27, 2013. Retrieved June 19, 2024. https://obamawhitehouse.archives.gov/the-press-office/2013/06/27/remarks-president-obama-and-president-sall-republic-senegal-joint-press-.
- ***. 2019. US Cloud Act. https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf.