Hacking the government: a comparative case study in Europe

To what extent do the national cybersecurity strategies of France, Germany, and Bulgaria address hack-and-leak operations?

Nicky Siebelt

S1468650

Master Thesis: Crisis and Security Management

Leiden University

Faculty of Governance and Global Affairs

Date: June 29, 2020

Wordcount: 18,769

Supervisor: Dr. Tatiana Tropina

Second Reader: Dr. James Shires

Index

List of abbreviations

ANSSI	Agence Nationale de la Sécurité des Systèmes d'information – The French National Cybersecurity Agency
BMI	Bundesministerium des Innern – the German Federal Ministry of the Interior
BSI	Bundesamt für Sicherheit in der Informationstechnik – the German Federal Office for Security in Information Technology
CPDP	The Bulgarian Commission for Personal Data Protection
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
DNC	(American) Democratic National Committee
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HLO(s)	Hack-and-leak operation(s)
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IT	Information technology
NCSS	National Cyber Security Strategy
NRA	National Revenue Agency (of Bulgaria)
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale – Secretariat-General for National Defence

Introduction

During the American presidential elections of 2016, several thousand emails of presidential candidate Hilary Clinton were leaked. With the use of phishing methods, the email account of the chair of Clinton's campaign, John Podesta, was hacked after which many files were published on WikiLeaks (Van der Horst 2016; Chang 2018). Experts argue that this hack-and-leak operation, also known as the Democratic National Committee (DNC) email leak, was aimed to influence the American citizens to prevent them from voting on Clinton (Masters 2018; Matishak 2018). Investigations pointed at the involvement of hacking group Fancy Bear, which is linked to the Russian government (Vilmer 2019, 31). Even though Russia never stated to be responsible for the attack, the interference became world news.

IT experts have been stressing the importance of adequate cybersecurity for the government for some time (Kottasová 2019). They claim that it is worrying governments do not keep their systems updated, considering the actual rise of cybercrime and other cybersecurity threats, combined with the government's access to sensitive and vulnerable information (ibid.). Furthermore, countries interested in the internal affairs of other countries, or people who are against the system, can easily hire hackers or download (free) hacking software to illegally access IT systems without the targeted country being aware of this (ibid.). After a hacker collects data and leaks this online, the files can have a significant impact on the government affected. For the upcoming years, it is expected that the number of cybercrimes will increase, including those targeting governments (Ramadani et al. 2018, 341).

In this thesis, the focus will be put on policy gaps in national cybersecurity strategies (NCSS) related to addressing hack-and-leak operations (HLOs). HLO is a form of cybercrime whereby hackers with a political motive hack and leak information of people, organisations, or governments to influence the public opinion. This phenomenon has frequently been occurring in the past couple of years, yet, it is barely mentioned in governmental documents or the academic literature, supposedly due to the recently developed definition. By analysing cybersecurity strategies of three countries, it can be determined which policy gaps are present in addressing HLOs. The research question for this thesis is, hence, as followed: *To what extent do the national cybersecurity strategies of France, Germany, and Bulgaria address hack-and-leak operations?*

To answer the research question, the first part of this thesis will contain a theoretical framework. In this chapter, the terms ‘hack’, ‘leak’, ‘data breach’, and ‘HLO’ will be explained to prevent confusion about definitions as these terms are used simultaneously throughout this thesis. The theoretical framework will indicate the characteristics and risks of HLOs. Furthermore, the gaps in policies addressing HLOs – or related topics – as suggested by the literature, will be outlined. The theoretical framework will conclude with the gaps found in the literature by the author. Following this chapter, the methodology indicates how the research question will be answered, which types of information are used, how the case studies will be analysed, and what the limitations of this research are.

After the methodology, the third chapter of this thesis will include three subchapters in which three case studies will be analysed. In these cases, politicians or government institutions were hacked, and their information was intentionally leaked. The first case is about the Macron leaks of 2017, allegedly executed by the Russians, where a HLO took place right before the final voting round of the French presidential elections to influence the voting pattern of French citizens. The second case study discusses a HLO executed by a young adult who hacked over 950 German members of parliament, several journalists, and celebrities. Supposedly this was executed because he wanted to show people that he was able to hack the government. The third case analyses the 2019 Bulgarian revenue agency hack, whereby the majority of the Bulgarian citizens were affected after 21GB of data was hacked and leaked by someone wanting the Bulgarian society to see how weak the government was. The aim of analysing these three cases is to indicate that HLOs can be executed by people who are not necessarily politically motivated but do want to change the public opinion about the government. To research this, an overview of each HLOs is given, and the three strategies are separately analysed. In these subchapters, the focus will be put on perceived threats by the government, the objectives in the NCSS covering these threats, and policy gaps as found by the author in order to determine whether HLOs are addressed in these strategies.

After the cases have been studied, they will be compared with each other in a discussion to find similarities and differences between the three cases. Pointing out these differences and similarities may give further insights into how countries prepared for the HLO and how it was impacted. Supposedly, this will be beneficial for the development of future policies. In the discussion, the findings of this thesis will be compared to determine how countries have responded to the HLO and which policy gaps are present in their current national cybersecurity

strategies (NCSS). In the conclusion, findings will be summarized, and the research question will be answered.

Chapter 1: Theoretical Framework

To answer the research question and prevent confusion about the terminology, the most relevant terms have to be specified. A hack-and-leak operation includes hacks and leaks, but there is a difference between this phenomenon and the terms 'hack', 'data leaks', and 'data breaches', which will be pointed out in this theoretical framework. After the definition of a HLO is set, the risks associated with it are explained. Due to the newness of HLOs, the gaps in policies according to the existing literature and gaps in the literature according to the author will be discussed.

Defining hacks

The first mention of the term 'hacking' was around the end of the 1950s by the Massachusetts Institute of Technology in a note about a meeting (Chandler 1996, 230). Initially, it entailed the feeling of pleasure in a work process whereby people look at open information, deconstruct a system, and share this with their community. It was perceived to be a clever way to circumvent the imposed limits set by the law or government (Zook and Graham 2017, 393; Davies 2018, 193). The definition turned from positive to negative as it became more frequently associated with people profiting from illegally obtained information from others by breaking into their computers (Chandler 1996, 230; Oh and Lee 2014, 1). With the development of new electronic devices that were used to hack others or were able to get hacked, the definition of 'hacking' changed. Nowadays, it is defined as a situation in which someone abuses their authority to illegally access an information network while using a computer or another information processing device (Oh and Lee 2014, 1-2; Freitas and Gonçalves 2015, 55). A hack is often done on purpose but is not always with the intention to change politics or get financial gain. The motivation of a hacker can differ from being bored, to showing others what the hacker can do, or for personal satisfaction (Garrett 2013, 8; Zook and Graham 2017, 393, 394; Davies 2018, 172, 189).

Defining leaks

A possible consequence of a hack is the release of data in the form of a data breach or a data leak. To prevent confusion, both terms will be explained. Data breaches are security breaches

leading to documents or information becoming public. This can be the consequence of a hack, an insider accessing information without authorization, or because of a human error when, for example, an unencrypted hard drive or computer gets lost or stolen (Daly 2018, 478; Shires 2019, 239). A data breach can happen either on purpose or accidentally but is not necessarily aimed at making information public. Data leaks, on the contrary, can be defined as purposely publishing or sharing confidential documents or information with the media or on the internet. This is often done in an informal way to keep the leaker anonymous. Furthermore, the leaks are done without the authorization of the owner of the information (Pozen 2013, 521, 534). The motivation of the person leaking information may differ. Whistleblowing is one example of a data leak with the aim to make abuse public. Another motivation is a so-called "ego leak", which is done with the intention to show others that someone is able to access certain information (Hess 1984, 77-78; Pozen 2013, 532). A policy leak also frequently occurs, for example, in the Netherlands during 'Prinsjesdag. On this day in September, the Budget Memorandum is presented, which includes the financial ideas of the government for the upcoming year (Parlement.com n.d.). Government officials leak policy ideas with the intention to prevent or help certain policies to get through congress (Hess 1984, 77-78; Pozen 2013, 532).

Defining hack-and-leak operations

By intimidation, the spread of propaganda, and the use of covert operations, states have been trying to influence one another for decades (Omand 2018, 5). Within the literature, several different terms are used to describe the phenomenon in which an external actor, often another nation, tries to influence politics in another nation. One of these terms, as given by Omand, is "cyber-enabled subversion and sedition" (2018, 8). This refers to a situation in which equipment, like a computer, allows a hacker to access websites or electronic devices to intercept data. In addition, the term 'doxing' describes a situation in which confidential information is stolen from a person, organisation, or government, and is published on purpose (Hansen and Lim 2019, 151). This is often done with the intention to "humiliate, threaten, intimidate, or punish" someone (Douglas 2017, 199). When combining parts of these terms, the term "hack-and-leak operation" (HLO), as mentioned in the article of Shires (2019), can be defined. The main elements of a HLO are intrusion and interference. It can, thus, be described as a phenomenon in which a hacker uses electronic devices to illegally access another

electronic device on purpose, with the aim to steal data and leak this information. It refers to politically motivated acts, executed by a state actor or non-state actor, with the desire to influence politics or to change the public opinion about a person, government, or situation (Shires 2019, 235-237). The information leaked can contain disinformation in order to create chaos or to make the targeted actor suspicious (Marwick and Lewis 2017, 27). In short, HLO consists of a hack followed by a purposely data leak to influence the (political) opinion of people.

Risks associated with HLOs

There are several risks related to HLOs. The first risk is related to the everlasting presence of data on the internet. With the implementation of the General Data Protection Regulation in 2016, the European Union (EU) tried to make the process of deleting personal files easier. In this regulation, the 'right to rectification' (art. 16 GDPR), and the 'right to erasure', also known as the 'right to be forgotten' (art. 17 GDPR) are included. As such, people have the right to access their information present online. When requested, the information should be removed from a website or database, for example, when the data is unlawfully processed (art. 17.d GDPR). But the enforcement of these articles is quite difficult; once data is uploaded to the internet, it is hard to permanently delete it (Newman 2015 507-508; Kulche 2019). After a HLO, data is often put on anonymous websites where other internet users can download the files. This allows the data to rapidly spread over the internet and makes it, hence, difficult for government departments dealing with this to find all locations of the data to erase it (Willsher and Henley 2017; Sheridan 2019).

Another risk related to HLO and illegal cyber operations in general is the relatively low probability of detection. As a consequence, few people get caught and sentenced for executing cyberattacks or other illegal digital activities (Leukfeldt 2017, 60). On the one hand, this is because of the lack of resources governments have in digital law enforcement (ibid., 61). On the other hand, it is expected that the constant developing technological possibilities the internet offers, decreases the probability of detection. New technologies allow hackers to create gaps in systems and remove their traces, which makes it difficult to trace back the executer of a HLO (Ramadani et al. 2018, 341).

Perhaps the biggest risk of HLOs is when people start to agree with the information, ideas, and ideology spread by them, especially when the leaked information is not true.

Research has pointed out that when rumours, or (fake) news are repeated frequently, people believe this information (Skurnik et al. 2005, 722-723; Lee 2014, 234). Even though this does not necessarily mean that people politically change their behaviour immediately, the goal of HLOs, to influence people, could be achieved relatively easily (Hansen and Lim 2019, 154, 155). This risk increases when the leaked information is widely supported or accepted within a country, when the citizens start promoting a certain ideology based on the leaked information, or when people start engaging in terrorist or criminal activities based on the information they have from the leak (Omand 2018, 18). When one of these situations occurs, governments experience a paradox. On the one hand, people have freedom of speech, which allows them to share whatever they want, except in certain situations. On the other hand, increasing foreign influence is not desirable for the targeted country (ibid., 19).

Policy gaps according to the literature

The literature points out that there are several gaps in existing policies that make it rather easy for hackers to engage in HLOs. One group of scholars argues that the gaps in policies are caused by the lack of a theory, which is related to the lack of knowledge. Security officers perceive cybersecurity in the light of the Cold War, where there is a constant – digital – threat between countries; states are waiting for the other nation to attack. This is not ideal, as cybersecurity is something intangible and attackers are able to infiltrate a system without the owner knowing it (Li 2010, 14, 15; Farell and Schneier 2018, 3). It is important to develop a theory based on technical security approaches and a theory of development: this will make it visible for people to see which technical security measures can be taken while the theory takes the technical developments into account. By creating a theory, solutions for a developing problem could be solved (Farell and Schneier 2018, 18-19; Moore 2018, 218; Beigel 2019 302-303).

Another school of thought states that the constant development of technological possibilities makes it possible for hackers to be ahead of the police or the governmental security agencies (Farell and Schneier 2018, 4; Vilmer 2019, 32, 42). A factor contributing to this is the lack of awareness and knowledge within governments (Oh and Lee 2014, 1,4; Omand 2018, 21; Vilmer 2019, 30, 32). Academics and experts have pointed out that humans are the weakest link in the ever-developing world of technology, as they do not know how to secure themselves (Kirkpatrick 2015, 23; Tsohou et al. 2015, 128-129). Governments do, however, try to prevent

problems. During the French elections of 2017, for example, political parties were warned about the possible interest of hackers in their campaign. As will be shown later, the email account of Emmanuel Macron got hacked; real and fake information was leaked even though the political parties were warned (Vilmer 2019, 42). It is also argued in the literature that laws and policies have become outdated because of a lacking definition for new phenomena as HLOs. The problem is not addressed appropriately in national or European legislation, which makes it difficult to punish these actions (Oh and Lee 2014, 5; Protrka et al. 2017, 87). Countries could learn from each other by comparing HLO situations of different nations, which allows them to create specific policies (Oh and Lee 2014, 1; Kirkpatrick 2015, 22; Shires 2019, 248). The best way to develop policies about this topic is by collaboration between different (international) government agencies. Also, by working together with internet companies, future attacks can be detected sooner (Omand 2018, 19).

Gaps in the literature

As a phenomenon, HLO is relatively new little specific literature is available about this form of digital threat. As a consequence, little information is available about policy gaps addressing HLOs or strategies to recognise or prevent HLOs. Furthermore, the existing literature mainly discusses politically motivated HLOs, while the examples of Germany and Bulgaria will indicate something different. In these cases, the desire for power or showing off one's IT skills has been a motive for engaging in HLOs. Based on the three case studies, it can be argued that an event can have the characteristics of a HLO, being intrusion and interference, but the hacker does not necessarily have to be politically motivated. This insight will add another dimension and, hence, another risk to the phenomena of HLOs.

Chapter 2: Methodology

As mentioned earlier, this thesis will analyse European HLO cases, whereby hackers might be politically motivated to influence the opinion of others (Shires 2019, 236). Comparing different cases will indicate policy gaps and will give further insights into how governments could respond to similar situations in the future. In this thesis, there will be looked at HLOs that took place in France, Germany, and Bulgaria, between 2017 and 2019. The three case studies will indicate what happened, how governments responded to the event, and which gaps in their NCSS might have led to this situation.

Data used

To answer the research question, several types of data will be used, including academic articles, media reports, blogs, and cybersecurity strategies from national governments. These sources all have limitations, mainly related to the bias of the author. To such prevent bias, the sources will be critically analysed and compared to each other. Official media outlets will be used to determine how a HLO is portrayed to society. To get more technical insights or access certain (technical) information about the three HLOs, cyber blogs or reports from security companies will be consulted. The aim is to link the information from these blogs to the other data sources to prevent bias. Analysing the NCSS will indicate what the national governments perceive as risks and how they want to protect their country against these risks. Comparing these strategies will show whether or not countries include hacking or leaking operations as risk, which will help to answer the research question.

Case study selection and design

The cases of France, Germany, and Bulgaria were selected because they are geographically located in Europe and are all three part of the EU. The latter makes it possible to analyse their national cybersecurity strategies (NCSS) and related cyber policies which countries share with the European cybersecurity agency ENISA. Several years ago, ENISA published a framework, the "NCSS Good Practice Guide", for European countries to design and implement their NCSS. Furthermore, these three countries are part of NATO, and all joined the Cooperative Cyber Defence Centre of Excellence (CCDCOE), which is aimed at improving the cybersecurity of

member states. France, Germany, and Bulgaria have created their own cybersecurity strategies that are based on national security interests and might be aligned due to them being part of the EU. The documents include the most important ideas and visions of the three countries towards cybersecurity and can give further insights into what situations or events countries expected to occur in the near future. Comparing the three NCSS will demonstrate how different countries in the same region respond to similar threats (Barlett and Vavrus 2017, 7).

There are also several other similarities and differences between the three cases. All three countries experienced similar situations in which information was hacked and leaked on purpose. The HLOs were aimed at politicians or governmental institutions. The motivation of the hackers and the responses of the government, however, differed in the cases. As for France, the aim was to influence French politics, while in the cases of Germany and Bulgaria, it seemed that young skilled people wanted to show that they disagreed with the way the government had been functioning. A second difference between the cases can be found in the response of the government. While all three countries set up committees researching the HLO, France and Bulgaria rapidly developed new policies and laws to prosecute those engaged in HLOs. In German politics, on the contrary, debates have been going on about whether the HLO was a consequence of security gaps or human error. The German Minister of Interior, for example, stated that the use of secure cybersecurity measures on an individual level might be more beneficial in preventing similar future events rather than creating new policies (Eddy 2019; Tiede et al. 2019). A final difference between the cases are the economic and social structures between France, Germany, and Bulgaria. It could be expected that these different structures may lead to another approach to handle HLOs.

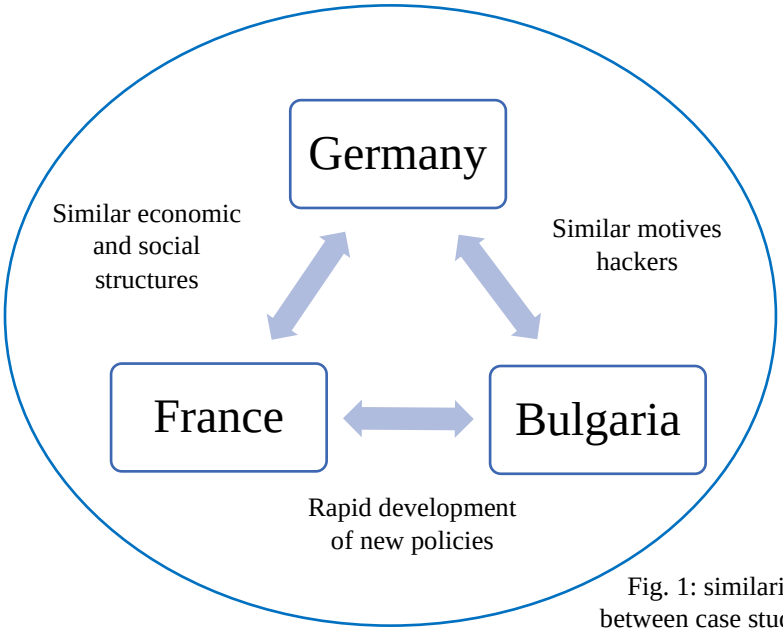

Fig. 1: similarities between case studies

In order to analyse the three cases in the same structural way, a comparative case study analysis will be applied, which will trace relevant aspects contributing to the HLOs. This form of researching case studies stresses the importance of researching the perspectives of the involved actors (Barlett and Vavrus 2017, 10). By analysing cases and the policy documents,

it will become clear how the event was portrayed by the media, how the government responded to it, and what is written about this topic in national strategies. This might point out different responses to a HLO. The case studies will be analysed horizontally and vertically, as explained in the article of Barlett and Vavrus (2017, 14). The horizontal analysis compares the actors, methods, and targets involved in this HLO. This will indicate who has been targeted, how, and what the intentions of the attackers were, which will show where attackers are interested in when executing a HLO. The vertical analysis compares the impact of the HLO on different levels of society (ibid.). Looking at the influence the HLO had on society or at the response of the three governments, for example, indicates how countries were (or were not) prepared for the HLO.

For all three cases, there will be explained what happened during the HLO, how the hack took place, who was targeted, and how much data got hacked and leaked. The second part of the case studies will deal with the person committing the hack-and-leak, which will show that state and non-state actors can be involved in a HLO. The third part analyses the media coverage of the incident and the response of the government after the event took place. This indicates whether the media and government perceived the HLO to be a severe threat to their country and if new policies were implemented to fight this threat. Analysing these topics will give insights into how other countries could respond to HLOs.

Limitations

When researching a relatively sensitive topic as HLO, several limitations are present. This thesis will focus on the publicly accessible documents of the three countries on the websites of ENISA and of the CCDCOE. These documents include national legislation, NCSS, and white papers about security policies, but the main focus will be put on the original NCSS. Not all European, neither French, German, or Bulgarian policy documents mentioning cybersecurity will be addressed. It must also be noted that these documents date from 2015 and 2016. As such, it is expected that several gaps in the NCSS are present due to increasing technological developments.

A limitation linked to accessing information is the lack of knowledge of the Bulgarian language. The author does, however, speak French and German, and can analyse documents in the original language. With the help of someone speaking Bulgarian, this language limitation will not be a problem in finding information.

Another limitation in this research is the relative recentness of the case studies and, hence, the policies or actions taken after the HLOs took place. The German and Bulgarian governments, for example, are still researching the incidents. Therefore, it is hard to determine what the (long-term) consequences of the HLO are and what impact the newly implemented policies have on the cybersecurity of the countries.

The final limitation is related to time and the geographical location of the author, which made it difficult to interview government officials from the case studies or to interview the potential suspects of the HLO. This, thus, means that the information in this thesis is mainly focussed on combining multiple digital sources.

Chapter 3: Case Studies

The case studies aim to indicate where the vulnerabilities lie before and after a HLO took place. They will be analysed chronologically, starting with the Macron email leaks of 2017, followed by the HLO of German politicians of December 2018 and January 2019. The final case study will discuss the Bulgarian tax agency hack of June 2019. Information in this chapter was found on the websites of ENISA and CCDCOE.[1] The NCSS available on these websites contain the original text in French, German, and Bulgarian, and, in the case of France, also contain an English translation.

After each case study description, the different NCSS will be analysed in order to find out whether HLOs are addressed. The threats perceived by the government, and the objectives aimed to counter these threats will be described. Gaps in the NCSS are pointed out, which indicates if countries included HLOs as a potential threat.

[1] For the original documents see: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map> and <https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies>.

Chapter 3.1: 2017 Macron email leaks

What happened?

During the French presidential elections of 2017, presidential candidate and current President Emmanuel Macron was targeted by a HLO. Between January and February 2017, Macron became a front-runner in the French elections; simultaneously rumours about the presidential candidate intensified on the internet (Vilmer 2019, 4). En Marche!, Macron's political party, stated that from December 2016 onward spear-phishing[2] emails sent to the campaign staff increased (Dickey 2017). Somehow, the attacker knew that the staff used Microsoft OneDrive to send emails and store information. As such, the hacker sent the employees emails that seemed official, in which they were asked to click on links that would go to a cloud or webmail (Guiton 2017).

Furthermore, the hackers used email spoofing[3] to trick the staff members into entering personal information and downloading official-looking documents. An example of this was an email coming from an address almost identical to the address of a staff member working with public appearances. The document was titled "some recommendations when talking to the press" and staff members were requested to download an attachment (Vilmer 2019, 11). Investigators suspected that this attachment contained malware that allowed the hackers to enter the campaign's computer systems (ibid.). Research indicated that the email providers and online clouds of five close colleagues of the president-elect were hacked by using the methods mentioned above. In total, 15 gigabytes (GB) of data, including approximately 21,000 emails and personal documents, were spread over the internet (WikiLeaks, n.d.).

According to Macron's political party, the data contained fake documents and false information, aimed to create disinformation and to put the political party in a negative light (Auchard and Felix 2017; Willsher and Henley 2017). An example of this was a rumour that

[2] Spear-phishing attacks are phishing attacks aimed at specific people, companies, or organisations. The intent is (often) to steal data from the targeted victim (Kaspersky 2020a).

[3] Email spoofing is a cyberattack whereby a seemingly trustworthy person sends an official-looking email with a request for personal information, financial transaction, or an attachment that should be opened by the reader. The cybercriminal aims to look like a familiar person or co-worker so that people do not question whether they should trust the sender. The emails can contain malware that gives the attacker access to the computer and network (Kaspersky 2020b).

Macron was collaborating with ISIS, which was spread after the documents were published (Vilmer 2019, 14). Media suggest that the hackers entering the different systems had been searching for missteps made in the past by Macron, which could be used to publicly shame him, so that people would not vote for him. As Macron was relatively young, 40 in January 2017, no infidelities in his background were found that could damage his reputation. Media expect that because of this, the hackers added fake documents to the leaked files to influence the voting of the French citizens (Grugq 2017; Willsher and Henley 2017).

On the 5th of May 2017, between 20:00 and 21:00, the documents were published on Pastebin[4] and 4chan.[5] Around 21:30, the information was picked up by WikiLeaks, after which #MacronLeaks became a trending topic on Twitter and was shared several thousand times (Vilmer 2019, 3, 13-14). At first, the Tweets were mainly shared by English speaking people, but during the night, the language of the Tweets shifted from English to French. In the morning, the topic was picked up by the French media, and it became breaking news (Nimmo 2017).

In France, 32 hours before the final voting round, 'election silence' forbids political campaigning. During this ban on election propaganda, candidates and political parties are not allowed to promote ideas, respond to comments, or win last-minute votes for a day and a half (Theviot 2013, 56, 58; Tambini 2017, 12; Willsher and Henley 2017; Vilmer 2019, V). Experts stated that the HLO was strategically planned, as the information was released two days before this election silence (Delerue 2019, 251). After the HLO became public news, Macron was, therefore, not allowed to respond to the situation (Willsher and Henley 2017; Vilmber 2019).

Who did it?

Due to the use of anonymous websites, it remained unclear who posted the information. It made people wonder if the hack was executed by the same people behind the HLO of the emails of Hilary Clinton during the American elections of 2016 (Willsher and Henley 2017).

[4] Pastebin is a website hosted on the deep web, where text can be shared or stored for some time. When using a VPN, people can share information anonymously. As a consequence, Pastebin is frequently used by people to share leaked information of data breaches (Ciarniello 2019).

[5] 4chan an anonymous online platform where people can share their opinions or pictures addressing different topics (4channel.org, 2020).

Academics have argued that it is, in this case, essential to look at three separate aspects of the event: the disinformation campaign, the hack, and the leak separately because they expected that this HLO was not executed by one person (Delerue 2019, 250). Most of the disinformation came from two different directions: from Russian media in France claiming that Macron was a "US agent" supported by a "wealthy gay lobby" (Sputnik 2017). Disinformation was also spread by American alt-right supporters, who are very active on social media and different forums. They suggested in Tweets and memes[6] that Macron participated in politically unjust activities and that he would actively support extreme Islamist groups (Harkinson 2017). According to Buzzfeed News, foreign supporters of Macron's opponent, Marine Le Pen, wanted to help her become president, which explains their online disinformation activities (Broderick 2017).

Experts and researchers argue that the Russian GRU, the country's military intelligence agency, is involved. APT28, also known as Fancy Bear or Pawn Storm, is a Russian cyber crew that had been collecting a lot of information about the French elections (Hacquebord 2017, 32). Furthermore, there were several similarities between the French HLO and the 2016 hack of the DNC, such as IP addresses and attack techniques (Noack 2017). Also, the content of some of the documents may lead to the suspicion that the hacker comes from a country where being homosexual is considered a scandal, like Russia. Several leaked documents pointed out that Macron would be secretly gay, but the sexual preferences of the president would not have had an impact on the LGBT+ respecting country (Vilmer 2019, 29). Former French Presidents François Mitterrand (1981-1995) and François Holland (2012-2017) both had affairs before and during their presidency; this did not lead to official removal procedures (ibid.). In France, the sexual preferences or activities of a president does not lead to him or her being forced to end the presidential term.

The French National Cybersecurity Agency (ANSSI) stated that it is also likely that the hack was executed by people inspired by the DNC case (Guiton 2017). The software used to change the files that were later spread over the internet, was mainly Russian, suggesting that the HLO was executed by the Russians. It could, nonetheless, be possible that the hacker wants to mislead people and make them think that this HLO was executed by a Russian. The person or group executing this attack might be linked to or inspired by the Russians, or they might

[6] A 'meme' is an image or video with text aimed to express a (political) opinion, or to make fun of a person or situation. The pictures are often created by individuals and posted on the internet (Brubaker et al. 2018, 741).

have had help from American alt-right movements, but it remains unclear who committed the well-planned hack. (Vilmer 2019, 21).

Media coverage

At the time the HLO became public, the government asked media outlets to behave responsibly as Macron was not allowed to respond. The French electoral commission led out a press release in which they recommended the media not to publish stories including the content of the leak on their websites (Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentelle 2017). Luckily for Macron, media waited until after the election silence as they did not want to influence the readers and voters with potentially fake news (Vilmer 2019, 39). The media were, however, allowed to address the issue; the government did not force or prevent them from writing about the topic.

While the executers of this HLO have not, yet, been caught, media and American intelligence officials immediately suggested Russian involvement (Auchard and Felix 2017; Hosenball 2017). Macron supporters argued the Russians did not have the intention to interfere in French politics with this attack but had the intention to show that they are able to get into the political systems of other countries as a symbol of power (Raulin and Gendron 2017). French government officials targeted by phishing methods also thought that the Russians were involved (Auchard and Felix 2017). Little to no discussions about other possible perpetrators were present in the media.

The response of the government

Cybersecurity was an important topic for the French government during the elections, due to the HLO taking place during the American elections of 2016 (Delerue 2019, 250). As such, a threat analysis was made in order to determine where potential threats could come from, after which the government declared that foreign interference in the French electoral process would not be accepted (Lausson 2017a and 2017b; Untersinger 2017; Vilmer 2019, 33).

After the elections and HLO, President Macron published a strategic review of the country's cyber defence in which the government stressed the importance of collaboration with the United Nations (UN) on international digital security (Delerue and Féry 2018). They called for international solidarity and action when the sovereignty of a state is violated by another

state on the digital domain and stated that countries should help targeted governments to prevent future foreign interference (ibid.). As the HLO violated the French Electoral Code, the government opened an investigation in collaboration with the French Police, but no conclusions have come out of it, yet (Vilmer 2019).

The government invested in the creation of an independent working group that wrote a report about information manipulation and identified vulnerabilities that could help other states that might experience foreign interference (in the future) (ibid, 43-44). Furthermore, in November 2018, legislation to tackle fake news has been created and passed through the National Assembly in which information manipulation is defined (ibid., 45). The authority responsible for the media regulation in France got control over the suspension over television channels that are controlled by foreign states if these states actively manipulate information, aimed to destabilize society. Violations of the authority's regulations may lead to imprisonment of one year plus a fine of €75,000 (Lecomte and Charlot 2019; Vilmer 2019, 45).

Even though the hack was executed well and included information to damage the political image of Macron, it did not have a significant influence on the French voters or the outcome of the presidential election. Structural factors, such as the regulation of the length of the presidential campaign and the regulated media environment in France, have had a positive effect on the minimal impact of the HLO on the French elections (ibid., 26). Furthermore, only thirty percent of French citizens believe what is said in the media, they are considered quite sceptical and are, hence, less vulnerable for people wanting to influence them (Bouvier 2016).

Research conducted by the Atlantic Council suggests that luck is also part of the minimal influence the HLO had on the elections because the hackers made several mistakes during the hack (Vilmer 2019, 27). It is expected that the hackers thought that the French were easily influenced by information about Macron supporting ISIS, due to the rising Islamophobia as a consequence of the terrorist attacks of 2015. As the French are relatively sceptical towards (social) media, the documents did not influence the voting pattern of the French (ibid. 27-28).

Another unforeseen aspect by the hackers and political polls was the chance of Macron becoming the French president, even before the HLO; the polls expected other candidates to have higher chances of becoming president (Hansen and Lim 2018, 162). After Macron became a political candidate, the hackers had a relatively short time to prepare and infiltrate the campaign. This differs from the DNC case, as it was already known on forehand that Hilary Clinton would be the Democratic candidate, allowing the hackers to prepare themselves before the elections begun, while they did not have this time to prepare for Macron (ibid.; Vilmer 2019, 28). A final unforeseen aspect is the relatively low level of English spoken by the French

(Ferrare 2017, 12). The leaked documents were mainly written in English and came from English websites, which most of the French citizens could or did not read until after it got in the news. It can be concluded that the French effective responsive strategy combined with the misinterpretations from the hackers, kept the damage on a minimal level (Vilmer 2019, 41).

Chapter 3.2: Analysis French NCSS

France has published its current NCSS in 2015. Even though the country had changed its strategy in the past after large cyber-incidents occurred, this did not happen after this HLO. In 2010, French financial and economic departments were spied on, and data was stolen. After this was discovered, the French government quickly implemented a new cyber strategy (SGDSN 2015, 7). In the past couple of years, the country has also developed other cyber strategies, such as the 2018 'Cyber Defence Strategy Review' and the 'Renewed Cyber Defence Strategy of 2019'. In these later documents, the threat of foreign digital interference is described as a potential risk to French national security (Ministère de l'Europe et des Affaires Étrangères 2017, 12).

In case of a cyberattack, ANSSI is the responding agency (SGDSN 2015, 20). They take preventative measures and are the first respondent during IT incidents that affect governmental institutions; they pay extra attention to this during the French elections. Political parties and electoral candidates are, however, responsible for their cybersecurity (Delerue 2019, 251).

Perceived threats by the government

The French NCSS discusses several threats that might have a negative influence on the country's national (digital)security. One of these threats is the lack of awareness: people do not have enough knowledge about cyber-attacks, which makes them attractive targets for criminals. Personal data theft has been rising the past couple of years; this form of cybercrime is easily executed after systems are illegally entered caused by the lack of preventative measures (SGDSN 2015, 7). The government expects that hackers or criminal organisations targeting these people are motivated by financial gain after personal data is sold on the internet (ibid., 20).

Besides for individuals, cyberattacks are also a threat to companies and the state, as this could have severe economic consequences (ibid., 3, 7). The French government expects that those targeting businesses or government institutions will try to illegally access their systems for a longer period of time, in order to steal different types of data. Allegedly, documents addressing economic plans from companies or political and military strategies from the

government are the most interesting for attackers. This information could allow attackers to interrupt activities within companies or society (ibid., 14).

The French government expects that mainly organized criminal groups engage in cyberattacks as blackmailing, sabotaging systems, or data theft from companies and the government. Espionage and data theft can, however, also be executed by foreign states, which has, according to the NCSS, led to political mistrust between countries (ibid., 38). The country recognizes that hackers can easily access unsecured or outdated networks. Neglected systems or careless employees that mix their private and professional life can have severe consequences depending on the data they are working with (ibid., 8). Due to the constant technological developments, currently available services, digital equipment, and electronic devices are not always up to date, and cannot avoid specific threats, such as data leaks (ibid., 31).

The government perceives disinformation to be another threat to society. After the terrorist attack of 2015, there was an increase in fake governmental websites aimed to influence the French public opinion towards the government (ibid., 7, 14). This manipulation method is described as a new technological development that could damage society. Related to this is the spread of propaganda and disinformation on social networks, which can profoundly influence the opinion and behaviour of people (ibid., 20). Terrorists are using social media to gather supporters and find volunteers that are willing to cooperate (ibid., 38). The increasing capabilities of hackers and the use of new hacking methods leaving little traces makes it difficult for authorities to find the executers (ibid., 8-9, 14).

A final threat the strategy describes is the increasing power of a small number of companies working with sensitive data. In France, several companies have access to a lot of personal data; this business oligopoly could lead to the abuse of power (ibid., 38). A risk could occur when personal data, for example, about healthcare, is stolen from companies processing this information, especially when it remains unclear who has stolen this information. Stolen healthcare data could lead to "abusive commercial exploitation," whereby insurance companies use the information to sell high insurances to people from which the health-related data was leaked (ibid., 21). To prevent economic destabilisation or the spread of propaganda based on personal information, the government wants to control this data and check on the companies that own the information (ibid., 8). Transparency within these companies should be increased so that people know what is done with their data (ibid., 30).

Objectives and measures in NCSS to tackle perceived threats

The French NCSS focusses on five objectives, including several sub-topics aimed to better the cooperation between different actors within the country. This cooperation will allow the French cybersecurity to keep improving (SGDSN 2015, B1).

The first objective discusses the importance of protecting critical infrastructure with digital means. The strategy stresses the need for trustworthy and well-functioning digital (security)tools (ibid., 14-15). To promote the development of such tools, the government wants the Expert Panel for Digital Trust to monitor newly developed cyber software, -services, and -products related to cybersecurity, but the panel has not been set up yet (ibid., 14). Furthermore, government documents related to digital security have to include an impact assessment addressing cybersecurity risks to prevent future problems (ibid., 15).

The second objective focusses on digital trust, and the influence cybercrime may have on France. Here, it is stressed that the French government should take the lead in spreading awareness about the damage propaganda, disinformation, and manipulation of information may have on society (ibid., 21). To assist people with cybersecurity issues, a platform was created where individuals and companies can get assistance with problems related to digital devices, internet, or social media accounts (SGDSN 2015, 21; Cybermalveillance France n.d.; ANSSI 2020). As there are little specific statistics about cybercrime, this website will also indicate the different types of cybercrime present in France, allowing the government to take adequate measures (ibid., 22). Also, the country wants to universalise regulations and help other countries with the development or improvement of their cybersecurity norms and frameworks in order to put an end to illegal digital activities (ibid., 23).

Awareness-raising for the entire country and more frequent cybersecurity education is the third objective of this NCSS. Especially people working within the government and businesses should participate in awareness-raising projects. As younger children and teens are also frequently online, the risks of cybersecurity should be more frequently addressed in educational programmes. It is expected by the government that these groups are vulnerable because they do not immediately recognize threats (ibid. 26-27).

The fourth objective is about technology companies and the internationalisation of cybersecurity products. To make sure business oligopolies do not abuse their powers, the small number of companies that produce cyber-goods and -services are monitored by the government. To create diversity on the market and prevent a monopoly, the government will

increase its investment in smaller cyber companies and will also promote the export of products made in this entire sector (ibid., 31, 34). The country stresses the importance of the involvement of the EU; they should not only buy European cybersecurity products but also globally promote them (ibid., 33). France wants to stimulate knowledge sharing within the private sector to create outstanding products, but also to prevent future cyberattacks aimed at these businesses. The government is allowed to intervene in businesses during a serious (cyber)crisis that might harm the country, but not during a crisis that only affects a small number of businesses (ibid., 31).

The final objective is about the leading French role in cyberspace. International trust should be established in order for countries and sectors to work together and develop safer and better cybersecurity products. The government, therefore, wants to invest in international forums where technicians and academics combine their knowledge and discuss cybersecurity-related topics with European policymakers (ibid., 39). With the help of France, countries can improve their cybersecurity capabilities; this will have a positive effect on the French cybersecurity, international relations, and levels of trust between the helped countries and France (ibid., 40).

Policy gaps

The literature review pointed out several policy gaps that are often present when addressing HLOs. It seems that the French government is aware of these gaps, such as that new technological developments might form a risk (SGDSN 2015, 13). Furthermore, they frequently create new and specific cyber-policies, which have to address potential risks (ibid., 15). Additionally, France wants to promote cooperation between countries to prevent future attacks and has, as such, been cooperating with Germany (ibid., 33-34).

There are, nonetheless, issues that are not addressed by the NCSS. The first gap is the lack of implementation of awareness-raising measures within companies, governments, and on an individual level. The French government argues that it is the responsibility of all the French people to protect themselves against cyberattacks (SGDSN 2015, 8). As shown, the HLO was caused by individuals close to Macron, who probably clicked on fake links in emails or downloaded files with malware, giving the attackers entrance to systems (Ouest-France 2017). While the team of En Marche! was warned about possible (foreign) interference, the head of IT of the team stated that people might have been tempted to bypass security procedures. People accessed their private email servers to send information that should have been sent with their

professional and secured email servers (ibid.). It remains unclear how seriously companies, the government, and individuals take the objectives addressing awareness-raising. This, hence, indicates that while the strategy stresses the importance of increasing awareness, implementation of these objectives is essential in preventing HLOs. It must be noted that after the HLO occurred, the government started to organize awareness training and crisis exercises for people working in the government, in order to prevent future cyberattacks (Ministère de l'Europe et des Affaires Étrangères 2019).

The second gap in this strategy is that the government expects that the companies that are part of the business oligopoly are the most likely to engage or be targeted by a HLO because they own a lot of data (SGDSN 2015, 21). The NCSS did not include the risk of the government being hacked and information being leaked, while they also have a lot of sensitive and valuable information that could, when stolen damage, the entire country when stolen.

The third gap is the lack of focus on threats coming from other countries. The NCSS discussed the threat of espionage executed by other states on governments and organisations trying to influence public opinion. The strategy did, however, not combine these threats or include the threat of foreign interference, especially during elections. As was shown with the 2017 HLO, foreign countries might be interested in influencing political processes by changing public opinion in their favour. The French strategy stresses that conflict "is increasingly being expressed in cyberspace", which has a negative impact on the levels of trust between countries (SGDSN 2015, 38). There is no further mention of this topic in the NCSS nor about how France will prepare itself against foreign interference.

Conclusion

The French NCSS describes threats coming from the lack of awareness within society; states and companies being interesting targets for cybercrime; the use of unsecured or outdated systems; methods to influence public opinion; and the abuse of power by powerful companies that have access to large data sets.

While the objectives (partially) cover all these topics, several gaps have been identified in this strategy. The first gap is related to the implementation of cybersecurity awareness-raising measures within society and within the campaign staff of President Macron. While the team was warned about potential threats, the use of unsecured email servers and human error have led to the HLO. Therefore, the government has been investing in awareness-raising

exercises to prevent future attacks (Ministère de l'Europe et des Affaires Étrangères 2019). The second gap is that the strategy does not cover the risk of the government being targeted with a HLO, even though they also have access to valuable information. The final gap is the lack of focus on threats coming from foreign governments wanting to influence political processes. It can be concluded that the French are aware of aspects of a HLO, but do not cover this in their NCSS.

Chapter 3.3: 2018-2019 German politics HLO

What happened?

Between December 2018 and January 2019, approximately 950 German politicians, several journalists, and celebrities had their data exposed on Twitter, making this one of the biggest hacks ever in Germany (Le Blond 2019; Götschenberg 2019; de Volkskrant 2019). The hacker published the stolen information in the form of an Advent calendar on his Twitter accounts @_0rbit and @_0rbiter. Every day, from the 1st of December 2018 until the 24th, he opened a "door" that contained real and fake information about the hacked people (BBC 2019a; Chase 2019a).

One of the victims was Chancellor Angela Merkel, whose email address and correspondence between others became public. Also, parliamentary groups such as CDU, SPD, and FDP, were targeted. A targeted Member of the State Parliament stated that apps on her phone reported that passwords of different social media applications changed several times per minute. A few days after her passwords changed, she found out that her information published on the internet (Amann et al. 2019). The hacked and leaked data of other politicians contained personal information, including phone numbers, credit card information, (home) addresses, private conversations, and email correspondence (BSI 2019, 9; de Volkskrant 2019; Le Blond 2019).

The information was gathered by hacking people's cloud services, social networks, and email accounts (BBC 2019a; de Volkskrant 2019). Many accounts had easy passwords as "iloveyou" or "1234", and were, therefore, easily accessible for the hacker (Eddy 2019; Schaake 2019). While the hacker had been publishing data since December first, the government officials noticed the leak in the first week of January, after approximately 17,000 followers, were able to access the published data (BBC 2019a; Götschenberg 2019).

Who did it?

German Minister of Justice, Katarina Barley, stated that the hack executed on purpose to influence the public confidence in democracy and German institutions (BBC 2019a; Tiede et al. 2019). At first, the Russians were seen as suspect because it was expected that they wanted to influence the upcoming German elections and the elections for the European Parliament

(BBC 2019a). Investigators of the hack thought, however, that the HLO was executed by a supporter of the German alt-right movement, as only the right-wing populist political party Alternatieve für Deutschland (AfD) had not been targeted by the HLO (Chase 2019b). This suspicion was confirmed as 3.4 GB of data of one specific TV satirist, Christian Ehring, was published (BBC 2019a). Allegedly, his data, including family vacation photos and personal details, was leaked because he won a court case in 2017 against Alice Weidel, the leader of AfD. In one of his shows, Ehring called Weidel a "Nazi slut," which she did not approve. The judge, however, argued that satire falls under the freedom of expression, which includes critical comments towards public figures. There was, hence, no punishment for Ehring (Saeed 2017). The relatively large amount of hacked and leaked information of Ehring and the AfD not being targeted made investigators suspect the involvement of (supporters of) the alt-right movement.

Only a few days after the HLO got in the news, 20-year old male Johannes S., confessed that he had executed it. The student did not work in a group, but as a lonely hacker, even though he had no professional computer skills. During a home investigation, no evidence was found that he supported a particular alt-right movement or political party (Chase 2019a and 2019b; de Volkskrant 2019). Two days after the HLO became public, the young male was arrested, but he was not held in custody as there was not enough evidence found against him (Eddy 2019). While he was considered to be a bored youngster by many, it was not the first time this student had been engaging in hacking activities. In 2017, for example, S. managed to enter the systems of the government and spy on them, which was noticed by the intelligence agencies. As he was underaged, his actions were not sanctioned (Bierman and Pole-Majewski 2019).

While the German police argued that his motivation was not political, the media claim that he hacked and leaked documents of (mainly) politicians, celebrities, and journalists on purpose to show people his irritation regarding the public appearances of these people. By sharing personal documents on Twitter, it is expected that he wanted to make his followers understand his annoyance and wanted to influence their opinion negatively about people whose accounts were hacked (BBC 2019a; Eddy 2019; Chase 2019b).

As he was not a trained hacker, he could also have been motivated by other factors, such as boredom or the fact that he was able to successfully hack people, which made him hack even more people (Taylor 1999). Young people who hack for fun or power are called "script kiddies" or "script kid". They intend to shock their victims, which gives them a feeling of

power. These young hackers are unaware of the possible outcomes of their actions or do not seem to care about the consequences for others (Bierman and Polke-Majewski 2019).

Media coverage

The German media described Johannes S., as a script kid who is technically a weak hacker but knew where to enter the system (Biermann and Polke-Majewski 2019). While the Federal police stated that he was not politically motivated, media suggest that his acts were motivated by right-wing thoughts (Reuters 2019). According to German media outlet Der Spiegel, the German public prosecutor's office had started three investigations against the online behaviour of S. before this HLO took place (Amann et al. 2019; Knobbe et al. 2019). Der Spiegel suggests that the hacker did not only publish the data because he was annoyed but also thinks that his acts were politically motivated as he had been spreading right-wing extremist ideas on the internet and approved right-wing hacktivists (Knobbe et al. 2019). On the forums he was active on, he mainly posted anti-Islam stories and articles about the importance of the return of the NSDAP. Furthermore, he frequently shared posts in which he stated to be against left-wing people. In one of his posts about migrants, he wrote: "The AfD will not get the whole clan away, so you need the NPD[7] to clean up properly" (Knobbe et al. 2019).

The response of the government

After the HLO became public, the National Cyber Defence Centre started coordinating and investigating the case. The BSI notified the victims of the HLO and advised them on the actions they should take. They located 50 websites and forums where the hacked data was published and requested to delete this information. The Twitter accounts used for sharing the information were also quickly blocked by the BSI (BSI 2019, 9). The HLO made the office acknowledge that people trying to influence public opinion do not necessarily have to come from a foreign country. In the country's NCSS, as will be discussed later, the focus is mainly put on threats

[7] The *Nationaldemokratische Partei Deutschlands*, or National Democratic Party of Germany (NDP) is a German political party that is considered to be a far-right party with an ultranationalist ideology. The party is described by opponents as a neo-Nazi party (Carter 2019; van der Ziel 2019)

coming from abroad, but this HLO made the German officials realize that there is more freely accessible and sometimes sensitive data on the internet than expected (ibid., 38).

While the government acknowledged the severity of the incident, they stated that the leaked information did not include critical information that could form a threat to national security. In a 2019 report about the national IT security situation in which this HLO is shortly explained, the BSI stressed the responsibility users have when using digital means. The office wanted to underline that people have to ask themselves how a hacker could get access to their files (ibid.). Interior Minister Horst Seehofer stressed the importance of the human factor in cyber incidents. He pointed out that it is, for example, important to use strong passwords and two-step verification, and questioned whether new legislation would prevent future attacks (Eddy 2019; Tiede et al. 2019). While several government officials agree with Seehofer, the government has been working on new cybersecurity law, including fines for specific actions (Beucher and Utzerath 2019).

The fact that this HLO took place could be considered as a surprise, as in 2015, the German parliament was hacked. The goal was to gather as much German intelligence as possible, in a very short time (Netzpolitik 2015; BBC 2016). The information, however, seemed to be collected for other purposes than leaks. Also, the German IT networks of the Ministries of Defence and Interior were repeatedly hacked in 2018 (DW 2018). German intelligence authorities found links between the experienced hacking group APT28 and the cyberattack of 2015 (Neuman 2018; Connolly 2020). In the past decades, these hackers participated in a wide range of hacks on foreign countries and their military institutions, including NATO and the American White House (Hacquebord 2015; Netzpolitik 2015). The Russians have denied any involvement in these two cases, making it difficult to determine who executed the hacks (Netzpolitik 2015; BBC 2016; Connolly 2020). These examples indicate that even if hacking operations seem to be solely for intelligence collection, vulnerability to hacks can lead to vulnerability to leaks because hacking is the first step of a HLO. In May 2020, Chancellor Merkel stressed that hybrid warfare and disinformation campaigns are becoming a more significant threat to the country and should no longer be ignored (von der Buchard 2020). She wants Russian digital activities within Germany to be monitored to prevent future similar cyberattacks (Conolly 2020).

Besides monitoring for foreign interference, police officials stressed the importance of stricter laws to fight digital crime. The president of the Federal Criminal Police Office stressed

the influence hackers could have on society and the damage they can do under the current mild laws. He pointed out that in 2016, over 83,000 cybercrime cases took place in Germany that cost approximately 51 million euro (Shalal and Jasper 2017). The 2019 HLO raises questions about German institutions dealing with cybersecurity; a member of parliament called for action after he thought hackers gained access to his email and social media account, right before the HLO took place. The organisations, however, argued that it was just one incident that would have little consequences for other members of parliament (de Volkskrant 2019). Due to the hacks taking place and the recent HLO, the call for the resignation of Minister Seehofer increased. Seehofer, on the contrary, argued that his resignation is not necessary as little critical data has been stolen (Chase 2019b; Eddy 2019).

Chapter 3.4: Analysis German NCSS

Since 1991, the German government has been working on national cybersecurity strategies. The country has put a strong focus on protecting critical infrastructure and on societal strategic issues on the digital domain, including the country's economy, society, and cultural interactions that were taking place online (Schallbuch and Skierka 2018, 3, 5). The most recent NCSS was implemented in 2016 in which the government stresses the importance of protecting the country, its industries, and its citizens (Bundesministerium des Innern (BMI) 2016, 8).

In case of a cyberattack, the Ministry of Defence, the Federal Office for Information Security (BSI), and the Bundeswehr (the German federal defence forces) have the responsibility to act (Federal Ministry of Defence 2016, 38). There are several other centres and teams involved in addressing cybersecurity. To improve the cooperation between incident response teams and the German authorities, the National Cyber Defence Centre was created in 2011, which has to report to the Information Security Office (Cyberwiser 2018). In 2017, the country's government opened an independent surveillance agency, ZiTiS, to prevent future attacks on the government and related institutions, they report to the Ministry of the Interior (Trimborn 2017). The CERT Bund, the German federal computer emergency response team, has to prevent and respond to security incidents in computer systems. The German government stresses, however, that cybersecurity is not the responsibility of one specific ministry or department, but that it is a "whole-of-government task" (Federal Ministry of Defence 2016, 36).

During a cyber-crisis, the involvement of governmental institutions with different and sometimes overlapping tasks has led to questions about responsibility. The Ministry of Defence is, for example, responsible for acting during a cyber-crisis with "defence aspects" while the BSI and Bundeswehr should be the first to respond during an attack aimed at critical infrastructure (Schallburch and Skierka 2018, 38). However, little information about what is meant by a "cyber-crisis with defence aspects" is found. According to Schallburch and Skierka, this has led to confusing situations whereby institutions did not take the responsibility they should have taken, and it might lead to future issues not being solved quickly (2018, 53).

Perceived threats by the government

In Germany, cyberattacks are taking place more frequently and are becoming more complicating due to the rising technological skills and professionalism of the preparators (BMI 2016, 7). This is a consequence of the digitalisation of the country, as many government- and commercial institutions, and individuals, store (personal)data on the internet, including information that might be interesting to attackers. Within the NCSS, several threats perceived by the government have been listed.

The document acknowledges that Germany is an interesting target for cyberattacks due to the dependence on digital infrastructures (BMI 2016, 7). All sectors in society are connected to the internet and use it constantly. Therefore, there is a lot of valuable data present on the internet that might be of interest to people with malicious intentions. The German government expects that the majority of the attackers have a background related to organised crime, are motivated by extremist or terrorist ideologies, or have a background in intelligence operations and, thus, work for a foreign government (ibid.). These groups are allegedly interested in information about German defence strategies or personal data of German citizens. By using digital means, these attackers do not have to be physically in Germany, which makes it difficult to arrest those responsible for an attack (ibid.).

The German strategy discusses the specific risks of attacks against state institutions and departments. By spying on administrative institutions or departments focussing on the armed forces, attackers can gather a lot of data about German (military) strategies, which form a threat to the country (BMI 2016, 7). Sabotaging information, spreading disinformation, and manipulating the public opinion, forms another risk to German society. The NCSS stresses that influencing the opinion of the people might lead to long-term risks and consequences for de liberty of the German citizens and democracy in the country (ibid.).

In this strategy, the threat of hacks and the threat of people trying to influence the public opinion, are covered, which are two aspects of a HLO. Hacking is, however, merely described as an intrusion into systems, and there is no explicit recognition that leaks can follow hacks, which can have severe consequences for the German state, companies, and society.

Objectives and measures in NCSS

The current NCSS includes four objectives to protect German digital security. The first objective is to take safe and self-determined actions in a further digitalizing environment, which includes improving the security of electronic identities, investing in IT security research, and increasing knowledge about cybersecurity (BMI 2016, 10). Awareness-raising is an important aspect of this objective: all users should be educated about the consequences of inadequate cybersecurity measures (ibid., 13-14). Furthermore, the government expects that the improvement of IT structures, products, and services, will lead to more transparency within companies (ibid., 17). The second field of action is the cooperation between the private and public sector. To create trust between sectors, a platform must be created where companies and the government share cyber-related information (ibid., 10).

The third objective focusses on the state-wide architecture of cybersecurity and how this can become more efficient and sustainable (BMI 2016, 10). The government should keep up with rapid technological developments, which could also prevent future attacks (ibid., 7, 35). This will be achieved by, for example, the creation of "early warning systems against cyberattacks from abroad" or by the further development of laws about cyberspace (ibid., 10). Furthermore, the country wants to invest in the National Cyber Defense Centre, as this institute has the responsibility to locate threats occurring inside the country (Lambrecht 2011). While it was expected that this organisation would publish information or reports addressing the HLO of 2018-2019, they do not have a publicly available website. Furthermore, the most recent information about the Centre on the website of the Ministry of the Interior dates back to January 2019 but does not include information about the HLO. Other governmental institutions addressing cybersecurity-related incidents, such as CERT-Bund or the IT Crisis Reaction Centre, do also not contain any specific reports about the HLO.

The final objective of the NCSS is the active position of Germany in the development of cybersecurity policies on a European and international level. By cooperation regionally and internationally, cyber capacity will be built, which will be beneficial in improving the German, European, and world-wide cybersecurity (BMI 2016, 10). Due to the digitalising world, it would, according to the strategy, be better to align national cybersecurity measures to the European ones. The country would like to help other countries in the development of cybersecurity policies and legal frameworks. Better European protection and resilience will lead to more and better protection for Germany (BMI 2016, 39). The country argues that NATO

should develop cyber-defence policies; Germany would like to have an active role in this process. Due to the emerging and increasing threats coming from, amongst others, hybrid warfare and foreign interference, the German government stresses the importance to keep strengthening NATO (ibid., 21).

Policy gaps

The German government seems to be aware of the gaps given by the literature review. The country acknowledges the need for awareness-raising within society (BMI 2016, 13-14), and that they should keep up with technological developments to prevent future attacks (ibid., 7, 35). They frequently update laws and policies addressing cybersecurity and are willing to cooperate with other countries to create better cybersecurity measures and frameworks (ibid., 10, 39). After analysing this document, three policy gaps related to how the country addresses HLOs have, however, been found.

The first gap is that this NCSS mainly focusses on threats coming from outside Germany. In the 2011 German NCSS, however, it was stated that cyber threats were not only coming from outside the country; cyber-attackers might also be present within the country and the former NCSS stated that these attackers could form a threat to national security (Federal Ministry of the Interior 2011, 3). The former strategy acknowledged that with the use of certain technologies, for example, a VPN,[8] attackers can locate their IP addresses outside Germany, making it difficult for the German government or police to find the attacker (ibid.). The current strategy does not mention the risk of people inside the country trying to attack the government. It remains unclear why this is excluded from the latest version of the NCSS. It must be noted that in a 2019 report, the German officials recognized that this is one of the gaps in their policies (BSI 2019, 9). They do, nonetheless, not mention whether they are going to address this in future policies.

Another gap in the NCSS is that there is no mention of measures to increase cyber awareness within the government. The strategy stresses that all internet users should have some knowledge of cybersecurity, but mainly discusses how the federal and state governments should implement cybersecurity awareness training students (BMI 2016, 13, 14). When

[8] A Virtual Private Network (VPN) is "a private computer network within a larger network such as the internet" (Cambridge Dictionary 2020).

graduating, they should have a basic knowledge of cybersecurity and related risks. This will, according to the NCSS, prevent future cyberattacks (ibid.). The German strategy does not mention any form of cyber awareness training for people working within the government. As was shown with the HLO, government officials are not aware of the importance of strong passwords. On the internet, certain websites can estimate the password-cracking time; the password "1234" can be cracked in 0.19 milliseconds (BeterBuys 2020). When using the right tools, hackers can hack several passwords per second, but using a strong password could reduce the chance of getting hacked (Channell 2019), which will, as a consequence, decrease the change of a HLO.

The third gap in the strategy is related to the lack of implementation of transparency requirements for government institutions about security incidents, such as a HLO. The German NCSS points out that companies have to become more transparent, as this will lead to the improvement of IT products and services (BMI 2016, 17). Furthermore, they stress the importance of sharing information about cybersecurity between companies and the government, which could help to prevent future incidents (ibid., 10). The HLO of 2018-2019 is, however, not mentioned on the websites of the government departments dealing with cybersecurity, even though it was expected that detailed reports would be published. This information could help companies, (state) institutions, or individuals in taking adequate measures to prevent future HLOs. It must be noted that this information might be missing because the government is still investigating the event and does, hence, not want to publish information that might turn out to be false.

Conclusion

In this chapter, the German NCSS was analysed to determine if the strategy addresses HLOs. It is interesting to note that the German Ministry of Defence is responsible for cyberattacks, which is not the case in the other case studies. The strategy is, thus, military-oriented rather than civilian aimed. As for addressing policy gaps, it can be concluded that this has been done partially. The German NCSS acknowledges that spreading (false) information that might influence or change public opinion within society is a significant threat to the country (BMI 2016, 7). The NCSS does, however, not address the risk of someone inside the country wanting to influence the national political debate. This was, nonetheless, included in the former German strategy. By only focussing on foreign threats, the government might miss signs of cyberattacks

executed within the country. Furthermore, the strategy stresses the importance of increasing awareness among students but does not include awareness-raising activities for government officials. As was shown with the HLO, the use of weak passwords can lead to personal details being hacked and leaked. The final gap found in the German NCSS is the lack of implemented transparency requirements for the government. The strategy points out that companies should increase their transparency, as this would lead to the improvement of products and services (BMI 2016, 17). Sharing knowledge between sectors would also lead to the prevention of future cyber-attacks. While the NCSS describes the role the government has in this objective, little documents about the technical details of the HLO were found. It is, however, possible that the government is still investigating the event.

Both the hack of the German Parliament of 2015, 2018, and the HLO of 2018-2019 show the continuing threats that large-scale hacks can pose to the German government. It is important that the country addresses this threat with appropriate policies and legislative measures. On the one hand, the government would like to become a leading country in protecting the EU and NATO. On the other hand, it could be questioned if the country is able to protect itself (BMI 2016, 10, 26, 39). Related to this is the focus of Germany on the EU and NATO member states. The German NCSS underlines the importance of strengthening these intergovernmental organisations as if they do not want certain countries to be involved in this process. The offensive cyber-programs from Russia could be a possible explanation for this. By intercepting, sabotaging, or influencing critical infrastructure, NATO, American, and Dutch governmental departments perceive Russia to be a threat to Europe (NCTV n.d.; NCSSIC and FBI 2016; Stoltenberg 2019).

Chapter 3.5: 2019 Bulgarian revenue agency HLO

What happened?

In June 2019, millions of Bulgarian citizens and businesses were affected by a data leak after it was stolen from the Bulgarian National Revenue Agency (NRA). A hacker was able to enter the system through a vulnerability in the Value-Added-Tax service on the website of the NRA. This service was not frequently used by the government or taxpayers and was, as such, not regularly updated (Nidecki 2019). The attacker used an SQL injection to enter the system. This method is perceived to be a relatively easy web hacking technique to gather data about users logging into the system or information present in databases. SQL injections are, however, easily spotted if the software is updated frequently or when penetration tests are executed (O'Neill 2019; Portswigger 2020). As the Bulgarian government did not execute regular security checks, this SQL injection led to the hack of the NRA, after which the data was leaked. At the end of June, the NRA discovered that someone had been trying to access the system without authorization but did not perceive this to be an urgent threat (Mediapool 2019a).

The 21GB leaked information included personal details of approximately 6 million Bulgarians, from which 4 million people resided at that moment in Bulgaria, and approximately 2 million people had passed away (CPDP 2019, 42). The country has 7 million citizens, meaning that the majority of the inhabitant's personal information, such as names, bank account information, pin codes, home addresses, and income, became public (BBC 2019b; Bostock 2019; CPDP 2019, 42; Gotev 2019; Kottasová 2019). The hack also included files from EUROFISC, the EU's department in fighting fraud, about mechanisms aimed to target and share information regarding VAT fraud (Gotev 2019). It remains unclear what the long-term effect of this HLO will be on those involved.

After the hack became public, people were able to download the data files themselves as they were not removed from the internet at first (BBC 2019b; Cimpanu 2019; Kline 2019). It was online and available for download for approximately a month. In July, news media reported about the HLO for the first time, because someone with a Russian e-mail address sent it to different Bulgarian media outlets. The email stated that the sender had accessed 110 databases, including those containing critical information (Krasimirov and Tsolova 2019).

Who did it?

Shortly after the HLO became breaking news, several theories about the motivation of the hackers were developed. The government, for example, expected that the attack was politically motivated and executed by a foreign country or by someone collaborating with another government (Mediapool 2019a). The Ministry of Interior, Mladen Marinov, connected the HLO to the purchase of American fighter jets, which Bulgaria bought in 2019. While he stressed that he did not know who executed the attack, he thought that the Russians would feel threatened after this purchase, because this was the country's largest military spending since 1989 when the Communist rule ended (Kline 2019; Santora 2019). As a consequence, Mladen expected that the Russians would try to hack the government (Mediapool 2019a). Bulgaria has, however, close ties to Russia; the latter denied any form of involvement in the hack (Krasimirov and Tsolova 2019; Santora and Schmitt 2019).

The media, on the other hand, expected that the attackers were motivated to hack and leak files for financial gain. The more information a hacker collects, the more this data is worth on the dark web (Kottasová 2019; Santora 2019). Experts stated that the data from this HLO is worth approximately 200 million US dollar, which could explain the motive of the hacker (Santora 2019). Another theory within the media was that the attackers intended to create panic within the Bulgarian society; the HLO could, hence, be considered an act of terrorism (Bostock 2019; Gotev 2019).

A few days after the attack, a 20-year old employee of a cybersecurity company, Kristiyan B., was arrested because the computer and software used to execute the hack were similar to his computer and software. After his arrest, he was charged with the illegal acquisition of computer data and the spread of this information (Bulgarian National Radio 2019; Tronchev 2019). He was detained for 72 hours but released because of his clean criminal record, his good behaviour, and his young age (Bulgarian National Radio 2019; A. Dimitrova 2019; Kottasová 2019; Santora 2019). B. is, nonetheless, not allowed to leave the country until the investigation about this HLO is completed (Krasimirov 2019). At the time B. got arrested, the commercial director of the company he worked at (TAD Group), was also arrested but released due to the lack of evidence (5GmediA 2019; Europost 2019).

Besides B. and the commercial director, the owner of TAD Group, Ivan T., was also arrested. At the time B. stated that he was able to enter the NRA, T. alerted the authorities and, therefore, claimed to be innocent (Europost 2019). B., on the contrary, stated that he was put

under pressure and was threatened by his boss to execute the hack; this was also confirmed by testimonies of former employees of the company (Rafailovich 2019). The Bulgarian Specialised Criminal Court of Appeal eventually accused T. of instigating the attack on the NRA and leading an organized criminal organisation (Drumeva 2019; Krasimirov 2019). According to Bulgarian media, T. hacked companies and their websites and then forced them to buy his services from TAD Group (Europost 2019; Dnevnik 2019). T. was held in custody for half a year, as the judges decided that he was a threat to public safety. He was, however, released after his bail of 100,000 BGN (approximately 50,000 euro) was paid (Rafailovich 2019; Velikova 2020b).

Media coverage

After government officials reported that they had arrested T. and B., two different opinions about them were present in the media. Media reported that T. had been engaging in organized crime and cyberterrorism and was, hence, portrayed as a terrorist and a threat to national security (Drumeva 2019; Europost 2019; Novinite 2019; 5GmediA 2019). B., on the contrary, was seen as a hero. The media stated that he is a script kiddie motivated by the desire to show the Bulgarian citizens that the national cybersecurity was weak and "a parody" (BBC 2019b; Krasimirov and Tsolova 2019; information 2019) and to show them that the government was "stupid" (Cimpanu 2019).

This HLO was, however, not the first time B. engaged in hacking governmental institutions. In 2017, for example, he hacked the website of the Ministry of Education because he saw it as his duty to make the government and the Bulgarian people aware of the weak governmental cybersecurity. With the hack, B. showed how exam grades of people attending any school could be changed. He did, however, alert the ministry about the security gaps, and no charges were pressed. B. even received a letter of thanks from the ministry and a job interview invitation at TAD group (Bulgarian National Radio 2019; Bostock 2019; Kline 2019; Nova News 2019a). On his social media accounts, B. frequently criticized the way the Bulgarian government works. According to him, they use pirated and illegally obtained software by which they infringe on the copyrights of many companies (Nova News 2019a).

Society greatly supports the work of B.: he became an internet sensation and even has his own fan page on Facebook (Nova News 2019a). He is not perceived as a criminal, but rather as a young and intelligent man who has shown the state how significant its shortcomings are

in terms of cybersecurity and the protection of data (Nova News 2019b; Rafailovich 2019). Surprisingly, this opinion was also shared by the Bulgarian government. Prime Minister Boyko Borissov stated that "people like B. are just wizards with incredible abilities" (Kostadinov 2019). According to the Bulgarian PM, the incident gave the government further insights into which aspects of the government should be better protected, which services are vulnerable for hacks, and what should be improved to prevent future attacks (ibid.).

The response of the government

Even though Bulgaria is one of the poorest member states of the EU, the country has been trying to create a stable cyber domain for the past couple of years, by participating in cyber programs from NATO (Santora 2019). Experts claim that the government has a lot of knowledge about cybersecurity and is aware of threats coming, for example, from hybrid warfare, but they do not perceive viruses, phishing, or data breaches as a threat to national security (Kline 2019; Santora 2019; Santora and Schmitt 2019). After the HLO, the NRA publicly admitted that they did not have the right knowledge regarding cybersecurity, as they never took preventative measures, such as penetration tests, which indicates where the security issues lie (Santora and Schmitt 2019).

It is not the first time a Bulgarian government institution experienced a cyber-attack. In 2018, the Commercial Registry was hacked due to security holes. As a consequence, the system broke down, servers and backups were damaged, and the registry's website was offline for almost 20 days (Rafailovich 2019). This made Bulgarians consider the situation in 2019 very serious, because the government knew after the attack of 2018 that they had to do something about the flaws in the system but did not take security measures (Kline 2019; Kottasová 2019).

After the HLO of 2019, the Bulgarian Commission for Personal Data Protection (CPDP) quickly investigated the hack and published a report about it (Kottasová 2019). During the investigation, several technical and organisational flaws were found, which might have caused several security gaps, allowing the hacker to access personal data (CPDP 2019, 42; Stoyanova 2019). Furthermore, the CPDP found out that the government did have some rules about the protection of personal data and how employees should take care of this, but these rules were not explicitly formed and were not physically provided to the governmental officials (ibid.). According to this commission, more policies and adequate systems should be developed so that the government can provide sufficient electronic services to the Bulgarian people.

Besides policies, the country should invest in risk management, which will allow them to identify threats and responses to the threat (ibid., 34).

Several prominent government officials stressed the responsibility of the government in situations like this one. They stated that the government should invest in preventative measures against future attacks, and not make B. a national hero (Nova News 2019b). The development of specific penalties for situations like this one should be prioritized. According to them, the current problem is that the country does not have sufficient money to invest in cyber awareness training, which might lead to future problems (ibid.).

After the CPDP report was published, the government created several new rules and policies about the minimum requirements for information security (State e-Government Agency 2020, 1). This document includes, among others, assessment rules to check the security networks used by the government to prevent future attacks (ibid., 3). For the Bulgarian citizens, the government created a tool that allows people to check if their data was exposed during the HLO (Nap.bg 2019). Furthermore, the government argued that the NRA was responsible for the HLO and sanctioned them with a fine of 5,100,000 BGN (approximately 2,6 million euro) (BBC 2019b; Bostock 2019; CPDP 2019, 42; Kirk 2019).

The NRA, however, recently appealed the fine, due to the lack of security measures taken by the government. They acknowledge that they have made mistakes, but also stress that they t it is not fair to punish a victim with a fine (Nova News 2020). The trial between the government and the NRA started in February 2020 but has been postponed due to investigations the court needs to execute to come to a conclusion (BGNES 2020; Velikova 2020a). The tax agency also considers to file a civil case against B. and T., and the hosting servers used to publish the documents (Mediapool 2019b). The agency claims that B. and T. are the ones responsible for the data leak and should, hence, pay the fine of 5,1 million BGN (Stoyanov 2019). These trials have not started yet.

Chapter 3.6: Analysis Bulgarian NCSS

Bulgaria has well-developed internet infrastructure, allowing almost everyone to have constant access to the internet, which is interesting for cybercriminals (Privacy Shield n.d.). With a large amount of data available online, the country has been working on cybersecurity and implemented its current and first NCSS in 2016. The strategy is based on documents provided by ENISA, ICANN, NATO, and other EU member states (Simonski and Sharkov 2016, 2). This NCSS was called "Cyber Resilient Bulgaria 2020" and focusses on how the country can protect its people, companies, government, and critical infrastructure in a better way (Privacy Shield n.d.; Council of Ministers 2016).

The strategy includes three phases. The first phase took place in 2016-2017 and focussed on achieving a basic level of cybersecurity capacity (Council of Ministers 2016, 52). The second phase focussed on the further development of rules, systems, and responses to incidents; it started in 2018 and ended a year later. The final phase started in 2020 and is aimed to create a "cyber sustainable society" in which the government wants to establish adequate measurements that are in line with the EU and NATO. To make sure these goals are accomplished, the government appointed a National Cyber Security Coordinator who is in close contact with the Council of Ministers (ibid., 53-55). The document is valid until the end of 2020, and the country expects to achieve all objectives before the end date.

Decisions about how threats should be addressed are taken by the president, the Council of Ministers, and the Council on National Security.[9] In case of a cyber incident, the country's president, Rumen Radev, decides what should be done and could even declare a state of emergency in which martial law becomes activated. Guidelines, programs, and policy proposals addressing national cybersecurity are created by the government department of sustainable development. The Council of Ministers has the final decision in the creation of new policies, frameworks, or laws addressing cybersecurity. They are also the ones who frequently update the country's NCSS (Council of Ministers 2016, 18).

[9] The Council on National Security is an advisory council that includes the following people: "The President of the National Assembly; the Prime Minister; the Minister of Defence; the Minister of Interior; the Minister of Foreign Affairs; the Minister of Finance; the Chief of the General Staff of the Bulgarian Army and one representative of each parliamentary group." (President of the Republic of Bulgaria, 2012).

Perceived threats by the government

The NCSS stresses that cyberattacks form a significant threat to the country, as they can be executed from another country. Due to the complexity and possibilities the internet offers, it is not always possible to find the people executing a cyberattack (Council of Ministers 2016, 6-7).

According to the strategy, the use of Advanced Persistent Threat (APT) is increasing and forms a serious threat to Bulgaria. This cyber-attack is frequently used by governments or state-sponsored groups; it aims to gather valuable information, often from corporations and governments over a longer period of time (Ghafir et al. 2018, 349; Maloney 2018; Kaspersky 2019). The Bulgarian NCSS argues that APTs are mainly coming from totalitarian regimes, countries with relatively low democratic levels, or countries engaged in hybrid warfare (Council of Ministers 2016, 6). Another threat is the spread of propaganda, ideologies, and radical ideas by terrorists. They manipulate information to attract supporters and are mainly focussed on targeting ordinary citizens (ibid.). A final explicit threat mentioned in the NCSS is accidental human error, which could lead to misuse or leaking information from governments, companies, and individuals (ibid.).

The NCSS describes three specific risk scenarios that might have severe consequences for the country. These situations are mainly intending to destabilize the country by executing cyberattacks. The first scenario is the threat of hybrid warfare in combination with physical attacks from a foreign country against Bulgaria. Another threat scenario is the risk of a cyberattack taking place during an internal crisis, for example, during a natural disaster or when there are problems with the country's critical infrastructure. A final risk-scenario includes accidental cyber incidents or purposely executed attacks aimed at society or the country's private sector (ibid., 5-6)

In case of an attack, it is expected that this comes from organized groups, foreign governments or military intelligence organisations, terrorist groups, or people executing industrial espionage. It is stressed that their motivation might differ; they might be economically motivated or do it out of curiosity. People might also execute a hack as a form of protest against the country, society, government, or another sector. Furthermore, intimidation, fraud, and the spread of illegal documents, such as child pornography, are also considered to be motivations for hackers. The Bulgarian government does, nonetheless, expect that most cyber attackers are financially motivated (ibid.).

Objectives and measures in NCSS to tackle perceived threats

The Bulgarian NCSS includes nine areas that should be developed or improved before the end of 2020. These nine areas contain several objectives and goals but are mainly about setting up systems, frameworks, or developing methods to fight cybercrime. As the objectives overlap with each other, several objectives will be highlighted and explained.

The first three objectives mainly focus on how Bulgaria wants to establish systems to protect the country against cybersecurity risks. The fourth objective discusses that information sharing between the government and stakeholders should increase. By making the public and private sector work together, the country wants to promote the creation of common awareness strategies and standard methods to share sensitive information (Council of Ministers 2016, 34). These strategies will be based on how other countries deal with similar issues. To achieve this, the state recognizes that trust between the government, companies, and individuals is crucial (ibid.). A high level of trust will be beneficial when developing effective public-private partnerships, which will allow these sectors to create a "national cybersecurity network" (ibid., 39).

Related to the development of secure networks is the fifth objective, which focusses on the improvement and development of regulatory frameworks, and laws sanctioning cybercrime (ibid., 38). These frameworks will also be based on those of other EU countries and should include who is responsible for which situation to create efficient interaction between all internet users. With the creation of new laws, cybercrime should be investigated and detected more quickly (ibid., 39). A set of standards will be developed in consultation with the different sectors. The government wants to create regulatory packages, which will make it clearer per sector what form of cybercrime is considered illegal (ibid., 40).

Objective six, seven, and eight focus on how national security can be protected by fighting cybercrime, which can be achieved by creating awareness programs for the state, society, and companies. By researching effective preventative measures, emerging threats should be recognized sooner, which makes it possible for these different actors to anticipate the threats (ibid., 41). Again, the NCSS stresses the importance of cooperation between the private and public sectors and the need for updating and creating regulatory frameworks. By active participation of the involved actors, information sharing will increase (ibid.). Furthermore, the government expects that the stimulation of research about cybersecurity will prevent future attacks (ibid., 45).

The ninth objective focusses on international interaction and the role of Bulgaria in the international system when addressing cybercrime. In this objective, the importance of working with other countries and taking an example of them on a European and international level is again stressed. Furthermore, the country wants to guarantee its citizens a maximally secured internet access, but also promote human rights in cyberspace by, for example, fighting organized digital crime (ibid., 48). They want to achieve this by joining projects set up by the EU, NATO, and UN, but also by working closer together with ENSIA, Europol, and the European Defence Agency (ibid., 47).

Policy gaps

Throughout the Bulgarian NCSS, a significant emphasis is put on the development of frameworks and international collaboration so that Bulgaria can gather more knowledge about cybersecurity. It must be noted that the structure of the NCSS is complex and confusing: with 62 pages of text, this strategy is the most detailed one of the three case studies. Even though this is their first strategy, it could be argued that this length creates confusion. The objectives frequently overlap with one another, which makes it difficult to see differences between them. An example of this is the similarity between the fourth, the sixth, seventh, and the eighth objective, as they all state that transparency will help in the fight against cybercrime and that awareness amongst all sectors present in society should be increased (Council of Ministers 2016, 30; 40-47; 56). Eventually, the conclusions of these objectives are similar: only by working together, cybercrime regulations can be established. While it is not necessarily negative to repeat certain goals, several of these objectives could have been merged, as they focus on the same topic. This would also make this strategy more focussed and more comprehensive.

Also, there are several gaps visible after analysing this NCSS. The first gap is related to the focus on threats by the government. The Bulgarian government seems to have a lot of knowledge about cybersecurity and even includes specific risk scenarios, which the other NCSS did not include. This strategy focusses on large-scale cybersecurity threats and hybrid warfare. The literature review pointed out that countries are not focussed on threats coming from new technological developments. It is, however, interesting that this NCSS focusses on threats as APTs, but seems to underestimate or ‘forget’ the threat coming from relatively easy

hacking tools. Accidental data leaks are described as a risk, but the strategy does not include purposely executed hacks or leaks, even though this could also severely damage the country.

A second policy gap is the lack of focus put on cybersecurity attacks executed from within the country. The NCSS includes a risk-scenario about purposely attacking society or the state, but it seems as if the government puts the focus on attacks coming from abroad or terrorist organisations (Council of Ministers 2016, 5-6). The 2019 HLO indicated that hacks and data breaches are relatively easy to execute, do not necessarily have to be executed from abroad, and can lead to large amounts of data being leaked (Kleine 2019; Santora 2019; Santora and Schmitt 2019).

The final policy gap is related to the lack of taking preventative measures by the government. The HLO took place during the second phase of the NCSS, in which the focus was put on coordinated responses to cyber incidents and taking preventative measures (Council of Ministers 2016, 41). Research conducted after the HLO pointed out that the Bulgarian government did not take any preventative measures against cyberattacks before the HLO took place (Santora and Schmitt 2019). Furthermore, the government stresses the importance of creating awareness because this could prevent future attacks. Government officials have, however, pointed out that the government does not have enough money to invest in awareness-raising. While this is essential in the prevention of future attacks, it is questioned whether this objective will be achieved before the end of 2020.

Conclusion

The Bulgarian NCSS is very national oriented; the focus is on the development of frameworks, improvement of laws, and the creation of new systems to find those targeting Bulgarian interests. To achieve this, the public and private sectors have to cooperate. New policies will be based on international examples, as suggested by the literature review. It is questioned whether all objectives will be achieved or whether some objectives stay on a declaratory level. Bulgaria has high levels of corruption within governmental departments, which might prevent policies and laws to be implemented or executed (GAN Integrity 2017; Transparency International 2020, 22). On the other hand, after the HLO was investigated by the CPDP, the government quickly implemented new policies about information security to prevent future similar attacks.

The Bulgarian NCSS is quite long; several goals and objectives are repeated. As such, three policy gaps were found in this strategy. The first gap is about the focus put on large-scale cybersecurity threats, while relatively easy hacking methods are not discussed. These methods can, however, have severe consequences and a significant impact on the country, as was shown with the HLO. The second gap is the focus put on threats coming from abroad. This HLO indicated that hackers attacking the government can also be present within the country, while the NCSS mainly focussed on threats from terrorist organisations, hostile government, or criminal groups. The final gap is that the NCSS stresses the importance of taking preventative measures, even though the government did not implement such measures before the HLO. The strategy underlines the importance of awareness-raising activities, but government officials have stated that there is no money available for this objective, making is, hence, difficult to achieve this objective.

Chapter 4: Discussion

In this thesis, it was questioned to what extent national cybersecurity strategies address hack-and-leak operations. In order to answer the research question, three case studies have been researched whereby information was hacked and leaked from different governmental actors. In this chapter, aspects of the case studies and aspects of the NCSS analysis will be discussed.

Discussion: case studies

The case studies have shown several different aspects of hack and leak operations. There are differences between the potential damage a HLO can cause, the motivation of the hackers, the way the media covered the HLO, and the responses of the government.

The thee cases show how relatively easy hacking tools can gather a lot of data; damage could be done on a large-scale. The French case indicates how foreign actors hacked and leaked information to influence voting patterns. The German and Bulgarian cases show how hackers wanting to make a statement, can expose data of millions of people, also by using easy hacking tools. Both countries also experienced hacks before the HLO occurred, which indicates that countries may more frequently have to deal with hacking (and leaking) operations. With the rise of digital means, increasing online activities, and accessible online data, it is expected that influencing people, especially during elections, will increase. As such, it is crucial that this threat is covered in national strategies. These examples indicate that HLOs are returning phenomena, even though the motivation to execute a HLO might differ. While no severe consequences have occurred (yet) in Germany and Bulgaria, it is expected that the leaked information will be on the internet for a while and, therefore, might form a threat in the future.

According to the literature, the motivation of the hacker is an important aspect of a HLO. As such, a HLO is described as a politically motivated cyber-attack whereby information from (a) government (official(s)) is hacked and leaked on purpose to influence the public opinion (Marwick and Lewis 2017, 27; Omand 2018, 5, 8; Shires 2019, 235-237). This definition is mainly focussed on influencing politics, but the case studies have indicated other motives, and it is, thus, questioned whether the definition of HLO should be extended. The French case could be described as a ‘classical HLO’ whereby hackers tried to hack and leak information in order to influence politics. When looking at the German and Bulgarian cases

from a cybersecurity perspective, they technically fit the definition of HLO because information was hacked and leaked. The motivation, however, differs from the political motive as described in the literature, as the aim for influencing politics seems to be absent. While the media have suggested that the German hacker was politically motivated, hacker S. stated that he did it out of boredom; no clear political motive was present. The Bulgarian case shows that hacks can be executed for financial gain but can also become a HLO. The hacker stated that he wanted to show the people how weak the Bulgarian governmental cybersecurity was and, thus, leaked the information. The examples of this thesis indicate that hackers can be motivated by other intentions than merely political aims, as suggested by the literature. The cases are technically similar, and akin cybersecurity measures can be used to address HLOs, but they do not all fit the given definition. It is questioned whether the definition of a HLO should be extended or rephrased so that similar events that are not politically motivated also fall within the definition. This might also allow governments to take adequate measures to the different forms of HLOs in the future.

Technically speaking, these HLOs followed the pattern of information begin hacked and leaked afterward and are, in essence, similar. When comparing media coverage, it is shown that there are similarities in the discussions and speculations in the media and the public. The French media, public, and government quickly agreed on the involvement of foreign actors, allegedly Russian intelligence groups. The German and Bulgarian cases show differences between similar-looking hackers. The media described both hackers as script kiddies, but they were portrayed differently. German media seemed to argue that the hacker was lucky in his attempts to hack government officials by guessing their passwords. The Bulgarian media described the hacker hacking the NRA as a wizard and national hero, as he shed light on the lack of cybersecurity measures of the country.

Besides differences in media coverage, government response indicates that they acted quickly to the HLO but responded to different aspects. As for France, the government implemented a working group that wrote new policies addressing information manipulation and indicated the vulnerabilities in the French system (Vilmer 2019, 43-44). Similar initiatives were started by the Bulgarian government with the creation of the CPDP, which also quickly indicated security flaws in the governmental cybersecurity and made suggestions for policy changes (CPDP 2019, 34, 42). The Bulgarian policies were, however, focussed on security requirements for the government rather than addressing disinformation (State e-Government Agency 2020, 1). Both countries did include technical details of the HLO. Germany, on the

contrary, investigated the case but did not publish technical details about the HLO. The focus was put on the responsibility of the individual rather than on the responsibility of the government. While the HLOs are technically similar, the differences between the cases in media coverage and responses of the government indicate that countries do not handle HLOs in a similar way. It could, hence, be questioned whether there is a need for one standard European policy addressing these types of cyber threats. This could give countries the opportunity to learn from each other and prevent future cyberattacks.

Discussion: analysis NCSS

After analysing the three NCSS, several policy gaps in addressing HLOs have been identified. It is, however, interesting to note that most of the policy gaps, as suggested by the literature review, are covered by the NCSS. All three strategies, for example, discuss how policies should be updated frequently due to increasing technological developments. Furthermore, the strategies stress that countries should share knowledge about cybersecurity with NATO or EU member states to develop strong collective cybersecurity and fight cybercrime (SGDSN 2015, 33; BMI 2016, 10, Council of Ministers 2016, 45-47).

Some topics are, however, currently not covered by some or all strategies. The French NCSS expects that companies working with personal data could be targeted by a HLO or could execute this operation themselves because they have access to valuable information (SGDSN 2015, 21). Therefore, the French government argues that this sector should be monitored by them, while they do not acknowledge that the French government is also an appealing target for hackers due to their access to sensitive information. The German and Bulgarian governments acknowledge that their access to data is a vulnerability (BMI 2016, 7) and could be an appealing target for hackers (Council of Ministers 2016, 6).

A second gap is related to the implementation of transparency measures described in the German NCSS. The French and German strategies both specifically stress the importance of transparency from (commercial) companies. As for France, this transparency is important so that businesses with access to sensitive data do not abuse their power (SGDSN 2015, 38). The German NCSS focusses on how companies should increase their transparency levels to improve the development of IT products and services (BMI 2016, 17). Both strategies point out that information sharing on an (inter)national level is essential to prevent future crises

situations (SGDSN 2015, 39; BMI 2016, 10). The Bulgarian strategy explicitly stated that transparency from the government would be beneficial in fighting cybercrime (Council of Ministers 2016, 30; 40-47; 56). After the HLOs, the French and Bulgarian governments published publicly available reports. The French document included information about the vulnerabilities of the state and information manipulation, which was the aim of the French HLO (Vilmer 2019, 43-44), while the Bulgarian report focussed on the technical details of the HLO (Kottasová 2019). The German government did, however, not publish documents addressing the event. On the websites of institutions that should respond to German cyber incidents, no technical details about the HLO are found. Information about the event could give companies or individuals further insights into how they could protect themselves against similar situations. It can, however, be argued that transparency from the government side about cyber incidents is required to create transparency within a country.

The Bulgarian NCSS contains a gap with their focus on threats as APTs (Council of Ministers 2016, 6), while they did not include the threat of relatively easy tools to enter systems. As shown with the HLOs, these methods can gather large amounts of data that could negatively affect a country. While the other two strategies do not specifically address these examples, France acknowledges the risk of data breaches due to security holes as a consequence of neglected systems or outdated software (SGDSN 2015, 8). Germany stresses the importance of awareness of new technological developments that might lead to cyberattacks (BMI 2016, 7, 35).

A policy gap present in all three strategies is the focus on threats coming from outside the country, executed by terrorists, criminal organisations, or through hybrid warfare (SGDSN 2015, 20, 38; BMI 2016, 7; Council of Ministers 2016, 6). The three HLO cases indicate that cyberattacks can also be executed from within the country and should, hence, be included in the NCSS as a potential threat. Only the German government acknowledged this gap after investigating the HLO, but it remains unclear whether they are going to include this aspect in future policies (BSI 2019, 9).

Another overlapping policy gap is the implementation of cyber awareness measures within the government. The French NCSS acknowledges the threat of the lack of awareness amongst internet users (SGDSN 2015, 7). While the team of Macron was warned about security measures, they allegedly did not have enough knowledge about cybersecurity threats, as several people were targeted by phishing methods (Ouest-France 2017). It is questioned if the spread

of awareness was indeed executed by the government before the HLO occurred. The German strategy did not specifically mention the spread of awareness within the government. The government does, nonetheless, stress the importance of raising awareness within society, because large amounts of data of individual users are spread over the internet, which is considered a security risk (BMI 2016, 10). The use of short and easy hackable passwords indicates the lack of knowledge of German officials and other prominent Germans who were targeted. The Bulgarian NCSS perceives human error as a threat, as there is the risk of people accidentally abusing data, which might lead to the leak of (sensitive) information. They, therefore, stress the importance of taking measures to prevent cyberattacks (Council of Ministers 2016, 6, 41). But due to financial reasons, no preventative measures were taken to protect the NRA and prevent the HLO (Santora and Schmitt 2019). The HLO cases indicate that government officials did not take preventative security measures or were unaware of them, which gave hackers access to data, which was later spread over the internet.

Chapter 5: Conclusion

HLOs consist of hacking, leaking, and influencing the public opinion. The three national cybersecurity strategies address the first aspect of a HLO, hacking, in different ways. The French NCSS expects that hackers are mainly focussing on financial gain and, therefore, sell hacked personal information on the internet (SGDSN 2015, 7). The French strategy does not discuss the risk of the government being hacked. The German NCSS perceives hacking as illegally accessing systems and as a threat (BMI 2016). They expect that mainly criminal organisations, terrorists, or governmental intelligence departments are interested in hacking the government. The Bulgarian government also expects that hackers are financially motivated to hack data. Hacks towards the government are, according to them, mainly executed with advanced hacking methods which could have a large impact on the country (Council of Ministers 2016, 5-6).

Further divergencies in the national security strategies can be found in relation to another aspect of HLO: leaking. The French strategy states that data leaks could be a consequence of outdated devices and systems (SGDSN 2015, 31). A risk-scenario is included whereby companies use leaked data to sell products aimed at the people involved in the leak (ibid., 21), but they do not specifically address the consequences of hacked and leaked information. The German strategy does not mention the risk of hacked information being leaked, even though this could have a large impact on the security levels of German businesses, the government, and individuals. The Bulgarian government specifically mentions that leaking information from the government, companies, or individuals on accident, could be caused by human error (Council of Ministers 2016, 6). They do, however, not specifically mention that this could also be caused by a purposely executed hack rather than only a human mistake.

The goal of a HLO is to influence the public opinion in a country. All three NCSS perceive disinformation or the manipulation of information as a threat to society. The French government expects that manipulating is mainly used by terrorists to attract people and to change the public opinion of the French citizens towards the government (SGDSN 2015, 20, 38). The 2017 HLO, however, indicated that foreign countries might also be interested in influencing politics. The German NCSS recognizes the long-term effects of influencing the opinion of people with disinformation on democracy (BMI 2016, 7). They do, however, not specifically mention the danger of influencing the public opinion to influence German politics. The government acknowledges that people interested in influencing this opinion might be

present within the country; the threat, hence, does not necessarily have to come from abroad (BSI 2019, 38). The Bulgarian government also considers information manipulation by terrorists a threat to society (Council of Ministers 2016, 6-7). The country does not specifically discuss the threat of influencing the public opinion or politics, nor does the strategy include the possibility of people inside the country wanting to influence politics.

The analysis of these three cases indicates that a HLO does not necessarily have to be political. Hackers can also be motivated by the desire to show their hacking skills, as was pointed out in the cases of Germany and Bulgaria. Furthermore, the use of relatively easy hacking tools can lead to large data leaks, which could form a threat to national security. Finally, the different NCSS contain several gaps that should be covered; these strategies only partially address HLOs. While all three countries took security measures after the HLOs occurred, only time will tell whether these measures will be effective in preventing future HLOs. The large amount of exposed data after these incidents, indicates that HLOs do not have to be executed by skilled hackers, which forms a threat to countries.

The HLO cases indicate the present vulnerabilities in the European cybersecurity. Stress-testing governmental systems that are used during democratic processes, training in recognizing hacks, updating software, and regular security checks could lead to a decreased number of attacks on European and national institutions (Schaake 2019). Furthermore, cooperating and developing a common European strategy that is similarly implemented in all member states, might prevent future cyber incidents.

Bibliography

4channel.org. 2020. “What is 4chan?” *4channel.org*, accessed June 12, 2020.

5GmediA. 2019. “NRA Hacking Affects the Security of Dozens of Companies and Government Bodies.” *5Gmedia.bg*, accessed June 4, 2020, https://www.5gmedia.bg/4350/hakvaneto-na-nap-e-zasegnalo-sigurnostta-na-desetki-firmi-i-drzhavni-organi.

Amann, Melanie, Maik Baumgärtner, Felix Bohr, Jörg Diehl, Matthias Gebauer, Roman Höfner, Martin Knobbe, Roman Lehberger, Veit Medick, Ann-Katrin Müller, Marcel Pauly, Sven Röbel, Marvel Rosenback, Jörg Schmitt, Philipp Seibt and Wolf Wiedmann-Schmidt. 2019. “Der junge der sich Orbit nennt.” *Der Spiegel*, January 11.

ANSSI. 2020. “Lancement National de la Plateforme Cybermalveillance.gouv.fr.” *ssi.gouv.fr*¸accessed June 11, 2020, https://www.ssi.gouv.fr/actualite/lancement-national-de-la-plateforme-cybermalveillance-gouv-fr/.

Auchard, Eric and Bate Felix. 2017. “French candidate Macron claims massive hack as emails leaked.” *Reuters*, accessed June 11, 2020, https://www.reuters.com/article/us-france-election-macron-leaks/french-candidate-macron-claims-massive-hack-as-emails-leaked-idUSKBN1812AZ.

Barlett, Lesley and Frances Vavrus. 2017. “Comparative Case Studies: An Innovative Approach.” *Nordic Journal of Comparative and International Education (NJCIE)* 1(1): 5-17.

BBC. 2016. “Russia ‘was behind German parliament hack’.” *BBC.com*, accessed March 29, 2020, https://www.bbc.com/news/technology-36284447.

BBC. 2019a. “German politicians targeted in mass data attack.” *BBC.com*, accessed March 29, 2020, https://www.bbc.com/news/world-europe-46757009.

BBC. 2019b. “Data of ‘nearly all adults’ in Bulgaria stolen.” *BBC.com*, accessed April 1, 2020, https://www.bbc.com/news/technology-49015511.

Beigel, Rebecca. 2019. “Review: Democracy hacked: political turmoil and information warfare in the digital age.” *Journal of Cyber policy* 4(2): 302-303.

Ben Nimmo. 2017. “#MacronLEaks Campaign Hits Resistance.” *Madium.com*, accessed June 12, 2020, https://medium.com/dfrlab/macronleaks-campaign-hits-resistance-4fa490e4ae55.

BetterBuys. 2020. “Estimating Password-Cracking Times.” *Betterbuys.com*, accessed June 10, 2020, https://www.betterbuys.com/estimating-password-cracking-times/.

Beucher, Klaus and Julia Utzerath. 2019. “Upcoming Cyber Security Law in Germany is introducing severe fines.” *Lexology.com*, accessed May 23, 2020, https://www.lexology.com/library/detail.aspx?g=c005f078-b8cc-4be8-9ff8-f7b8a6fb43f3.

BGNES. 2020. “Тръгна делото на НАП срещу глобата от 5 млн. Лева”.” *BGNESagency.com*, accessed May 20, 2020, https://bgnesagency.com/bulgaria/тръгна-делото-на-нап-срещу-глобата-от-5/.

Biermann, Kai and Karsten Polke-Majewski. 2019. “Ein Schüler hackt das politische System.” *Zeit.de*, January 8.

Blond, Le, Josie. 2019. “German politicians’ personal data leaked online.” *The Guardian*, January 4.

Bostock, Bill. 2019. “A hacker broke into Bulgaria’s tax system and stole the details of every working adult in the country.” *Business Insider*, accessed April 1, 2020, https://www.businessinsider.com/hacker-steals-personal-data-every-taxpayer-bulgaria-2019-7?international=true&r=US&IR=T.

Bouvier, Gwen. 2016. *Discourse and Social Media.* London: Routledge.

Broderick, Ryan. 2017. “Trump supporters are pretending to be French to manipulate France’s Election.” *BuzzFeed News*, accessed March 29, 2020, https://www.buzzfeednews.com/article/ryanhatesthis/inside-the-private-chat-rooms-trump-supporters-are-using-to.

Brubaker, Pamela Jo, Scott Haden Church, Jared Hansen, Steven Pelham and Alison Ostler. 2018. “One does not simply meme about organizations: Exploring the content creation strategies of user-generated memes on Imgur.” *Public Relations Review* 44(5): 741-751.

Buchard, Hans, von der. 2020. “Merkel Blames Rusisa for ‘outrageous’ cyberattack on German parliament.” *Politico*, May 13.

Bulgarian National Radio. 2019. “Кристиян Бойков е задържан за хакерската атака срещу НАП.” *BNR.bg*, July 16.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2019. “Die Lage der IT-Sicherheit in Deutschland 2019.” Bonn: Bundesamt f”ru Sicherheit in der Informationstechnik.

Bundesministerium des Innern (BMI). 2016. “Cyber-Sicherheitsstrategie für Deutschland 2016.” Berlin: Bundesministerium des Inntern.

Cambridge Dictionary. 2020. “VPN.” *Dictionary.Cambridge.org*, accessed May 14, 2020, https://dictionary.cambridge.org/dictionary/english/vpn.

Carter, Leah. 2019. “650 demonstrators stop neo-Nazi NPD gathering in Lower Saxony.” *DW.com*, accessed May 17, 2020, https://www.dw.com/en/650-demonstrators-stop-neo-nazi-npd-gathering-in-lower-saxony/a-51768279.

Chandler, Amanda. 1996. “The changing definition and image of hackers in popular discourse.” *International Journal of the Sociology of Law* 24(2): 229-251.

Chang, Alvin. 2018. “How Russian hackers stole information from Democrats, in 3 simple diagrams.” *Vox.com*, accessed June 10, 2020, https://www.vox.com/policy-and-politics/2018/7/16/17575940/russian-election-hack-democrats-trump-putin-diagram.

Channell, Justin. 2019. “How Passwords Get Hacked.” *Securi Blog*, accessed June 10, 2020, https://blog.sucuri.net/2019/12/how-passwords-get-hacked.html.

Chase, Jefferson. 2019a. “German government hack presents media with dilemma.” *DW.com*, January 7, accessed March 29, 2020, https://www.dw.com/en/german-government-hack-presents-media-with-dilemma/a-46986255.

Chase, Jefferson. 2019b. “German hacker behind massive political data leak identified.” *DW.com*, January 8, accessed March 29, 2020, https://www.dw.com/en/german-hacker-behind-massive-political-data-leak-identified/a-46991625.

Ciarniello, Alex. 2019. “What is Pastebin and why do hackers love it?” *Echosec.nl*, accessed June 12, 2020, https://www.echosec.net/blog/what-is-pastebin-and-why-do-hackers-love-it.

Cimpany, Catalin. 2019. “Hacker steals data of millions of Bulgarians, emails it to local media.” *ZDnet*, accessed April 1, 2020, https://www.zdnet.com/article/hacker-steals-data-of-millions-of-bulgarians-emails-it-to-local-media/.

Commission for Personal Data Protection (CPDP) Bulgaria. 2019. “Годишен отчет на Комисията за защита на личните данни за 2019 г.” Sofia: Commission for Personal Data Protection.

Commission Nationale de Contrôle de la Campagne électorale en vue de l’Élection Présidentelle. 2017. “Recommandation Aaux médias Suite à l’attaqye informatique don’t a été victim

l'équipe de campagne de M. Macron." *CNCCEP.fr*, accessed March 29, 2020, http://www.cnccep.fr/communiques/cp14.html.

Connolly, Kate. 2020. "Russian hacking attack on Bundestag damagest trust, says Merkel." *The Guardian*, May 13.

Council of Ministers. 2016. "Национална стратегия за кибер сигурност - Кибер устойчива България 2020." Sofia: Council of Ministers of the Republic of Bulgaria.

Cybermalveillance France. N.d. "Assistance et Prévention du Risque Numérique au Service des Publics." *Cybermalveillance.gouv.fr*, accessed June 11, 2020.

Cyberwiser. 2018. "National Cyber Security Strategy – NIS Capacities." *Cyberwiser.eu/Germany-de*, accessed May 8, 2020.

Daly, Angela. 2018. "The introduction of data breach notification legislation in Australia: A comparative view." *Computer Law&Security Review: The International Journal of Technology Law and Practice* 34(4): 477-495.

Davies, Sarah, R. 2018. "Characterizing Hacking: Mundane Engagement in US hacker and Makerspaces." *Science, Technology, & Human Values* 43(2): 171-197.

Delerue, François and Aude Géry. 2018. "France's Cyberdefense Strategic Review and International Law." *Lawfare*, accessed 29 March 2020, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

Delerue, François. 2019. *Cyber Operations and International Law*. Cambridge: Cambridge University Press.

Dickey, Christopher. 2017. "Fighting back against Putin's hackers." *TheDailyBeast.com*, accessed June 8, 2020, https://www.thedailybeast.com/fighting-back-against-putins-hackers.

Dimitrov, Samuel. 2019. "Хакерът" Кристиян Бойков бил разкрит през Гугъл." *Mediapool.bg*, accessed May 19, 2020, https://www.mediapool.bg/hakerat-kristiyan-boikov-bil-razkrit-prez-gugal-news296395.html.

Dimitrova, Alexandra. 2019. "" Пуснаха на свобода Кристиян, обвинен за хакерската атака на НАП!" *TraffixNews.bg*, accessed May 19, 2020, https://trafficnews.bg/obshtestvo/pusnaha-svoboda-kristiian-obvinen-hakerskata-ataka-nap-148862/.

Dimitrova, Veronika. 2019. “САМО ПО NOVA: Говори обвиненият за хакерската атака срещу НАП (ВИДЕО).” *Nova.bg*, accessed May 19, 2020, https://nova.bg/news/view/2019/07/19/257426/само-по-nova-говори-обвиненият-за-хакерската-атака-срещу-нап-видео.

Dnevnik. 2019. “Собственикът на "ТАД груп" вече е обвинен за ръководител на престъпна група.” *Dnevnik.bg*, accessed June 4, 2020, https://www.dnevnik.bg/bulgaria/2019/09/12/3962748_sobstvenikut_na_tad_grup_veche_e_obvinen_za/.

Douglas, David, M. 2016. “Doxing: a conceptual analysis.” *Ethics and Information Technology* 18(3): 199-210.

Drumeva, Ina. 2019. “Съдът окончателно остави в ареста собственика на "ТАД груп" за кибертероризъм.” *Dnevnik.bg*, accessed June 4, 2020, https://www.dnevnik.bg/bulgaria/2019/09/13/3962921_sudut_okonchatelno_ostavi_v_aresta_sobstvenika_na_tad/.

DW. 2018. “Hack on German government network ‘ongoing’.” *DW.com*, March 1, accessed March 29, 2020, https://www.dw.com/en/hack-on-german-government-network-ongoing/a-42788536.

Eddy, Melissa. 2019. “German Man Confesses to hacking Politicians’ Data, Officials Say.” *The New York Times*, January 8.

European Parliament and the Council of the European Union. *GDPR: Regulation 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.* Regulation 2016/67. Brussels: Official Journal of the European union, 2016. Accessed April 25, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=NL.

Europost. “Head of TAD Group: I am taking down the government.” *Europost.eu*, accessed June 6, 2020, https://europost.eu/en/a/view/head-of-tad-group-i-am-taking-down-the-government-25999.

Europost. 2019. “Three charged with Revenue Agency hack.” *Europost.eu*, accessed June 4, 2020, https://europost.eu/en/a/view/three-charged-with-revenue-agency-hack-25890.

Farrell, Henry and Bruce Schneier. 2018. “Common-Knowledge Attacks on Democracy.” *Harvard University: Berkman Klein Center for Internet and Society* 7: 1-20.

Federal Ministry of Defence (Germany). 2016. “White Paper on German Security Policy and the Future of the Bundeswehr.” Berlin: Federal Ministry of Defence.

Federal Ministry of the Interior (Germany). 2011. " Cyber Security Strategy for Germany." Berlin: Federal Ministry of the Interior.

Ferrara, Emilio. 2017. "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election." *Information Science Institute University of Southern California*, accessed March 29, 2020, https://arxiv.org/ftp/arxiv/papers/1707/1707.00086.pdf.

Freitas, Pedro Miguel F. and Nuno Gonçalves. 2015. "Illegal access to information systems and the Directive 2013/40/EU." *International Review of Law, Computers and Technology* 29(1): 50-62.

GAN Integrity. 2017. "Bulgarian Corruption Report." *Ganintegrity.com*, accessed May 30, 2020, https://www.ganintegrity.com/portal/country-profiles/bulgaria/.

Garrett, Bradley, L. 2013. *Explore Everything: Place-Hacking the City*. New York: Verso Books.

Ghafir, Ibrahim, Mohammad Hammoudeh, Vaclav Prenosil, Liagxie Han, Robert Hegarty, Khaled Rabie and Fransicso J. Aparicio-Navarro. 2018. "Detection of advanced persistent threat using machine-learning correlation analysis." *Future Generation Computer Systems* 89: 349-359.

Gotev, Georgi. 2019. "EU anti-fraud network EUROFISC hacked in Bulgaria." *Euractiv*, accessed April 1, 2020, https://www.euractiv.com/section/cybersecurity/news/eu-anti-fraud-network-eurofisc-hacked-in-bulgaria/.

Götschenberg, Michael. 2019. "Hackerangriff auf Hunderte Politiker." *ARD*, January 4, accessed March 29, 2020, https://blog.ard-hauptstadtstudio.de/deutsche-politiker-gehackt-101/.

Grugq, Thaddeus, T. 2017. "A Last Minute Influence Op by Data DDoS." *Medium.com*, accessed March 29, 2020, https://medium.com/@thegrugq/a-list-minute-influence-op-by-data-ddos-3698906d8836.

Guiton, Amaelle. 2017. "En marche, cible des hackers de Fancy Bear?" *Libération*, accessed March 29, 2020, https://www.liberation.fr/futurs/2017/04/24/en-marche-cible-des-hackers-de-fancy-bear_1565016.

Hacquebord, Feike. 2015. "Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House." *Trend Micro*, accessed March 29, 2020, https://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/.

Hacquebord, Feike. 2017. “Two Years of Pawn Storm: Examining an Increasingly Relevant Threat.” TrendLabs Research Paper 1-41.

Hansen, Isabelle and Darren J. Lim. 2019. “Doxing democracy: influencing elections via cyber voter interference.” *Contemporary Politics* 25(2): 150-171.

Harkinson, Josh. 2017. “Inside Marine Le Pen’s “Foreign Legion” of American Alt-Right Trolls.” *MotherJones.com*, accessed March 29, 2020, https://www.motherjones.com/politics /2017/05/marine-le-pen-alt-right-american-trolls/.

Hess, Stephen. 1984. *The Government/Press Connection: Press Officers and Their Offices.* Washington, USA: Brookings Institution Press.

Higgins, Andrew. 2017. “Fake news, fake Ukrainians: How a group of Russians titles a Dutch vote.” *The New York Times*, February 16.

Horst, Arjen, van der. 2016. “Hoe schadelijk zijn de Wikileaks-onthullingen voor Clinton.” *NOS*, October 29.

Hozenball, Mark. 2017. “U.S. increasingly convinced that Russia hacked French elections: sources.” *Reuters*, accessed June 4, 2020, https://www.reuters.com/article/us-france-election-russia/u-s-increasingly-convinced-that-russia-hacked-french-election-sources-idUSKBN1852KO.

Kaspersky. 2019. “What is an Advanced Persistent Threat (APT)?” *Kaspersky.com*, accessed May 30, 2020, https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.

Kaspersky. 2020a. “What is Spear Phishing?” *Kaspersky.com*¸ accessed June 10, 2020, https://www.kaspersky.com/resource-center/definitions/spear-phishing.

Kaspersky. 2020b. “What is Spoofing?” *Kaspersky.com*, accessed June 10, 2020, https://www.kaspersky.com/resource-center/definitions/spoofing.

Kirkpatrick, Keith. 2015. “Cyber policies on the rise.” *Communications of the AMC* 58(1): 21-23.

Kline, Kaity. 2019. “Man accused of hacking Bulgaria’s tax agency isreleased and given lesser charges.” *NPR.org*, accessed April 1, 2020, https://www.npr.org/2019/07/21/743912780/ man-accused-of-hacking-bulgarias-tax-agency-is-released-and-given-lesser-charges?t= 1585744712759.

Knobbe, Martin, Marvel Rosenbach and Sven Röbel. 2019. “Staatsanwälte ermittelten schon dreimal gegen Tatverdächtigen.” *Der Spiegel*, January 1.

Kottasová, Ivana. 2019. “An entire nation just got hacked.” *CNN.com*, accessed April 1, 2020, https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html.

Krasimirov, Angel and Tscetelia Tsolova. 2019. “In systemic breach, hackers steal millions of Bulgarians’ financial data.” *Reuters*, accessed April 1, 2020, https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-steal-millions-of-bulgarians-financial-records-tax-agency-idUSKCN1UB0MA.

Krasimirov, Angel. 2019. “Bulgaria’s data breach suspect sent back to custody.” *Reuters*, accessed June 4, 2020, https://www.reuters.com/article/us-bulgaria-cybersecurity/bulgarias-data-breach-suspect-sent-back-to-custody-idUSKCN1UY2D3

Krik, Jeremy. 2019. “Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged.” *Bankinfosecurity.com*, accessed May 20, 2020, https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000.

Kulche, Peter. 2019. “Persoonlijke informatie van internet verwijderen.” *Consumentenbond.nl*, accessed April 25, 2020, https://www.consumentenbond.nl/internet-privacy/persoonlijke-informatie-van-internet-verwijderen.

Lambrecht, Matthias. 2011. “Hilfloses Kriegsgeschrei gegen Attacken aus dem Netz.” *Financial Times Deutschland,* June, 20.

Lanoszka, Alexander. 2019. “Disinformation in international politics.” *European Journal of International Security* 4(2): 227-248.

Lausson, Julien. 2017a. “Présidentielle: pourquoi François Hollande redoute des cyberattaques.” *Numerama.com*, accessed June 10, 2020, https://www.numerama.com/politique/232966-presidentielle-pourquoi-francois-hollande-redoute-des-cyberattaques.html.

Lausson, Julien. 2017b. “Cyberattaques: la France se dit prête à riposte en case d’ingérence pendant la présidentielle.” *Numerama.com*¸ accessed June 10, 2020, https://www.numerama.com/politique/233185-cyberattaques-la-france-se-dit-prete-a-riposter-en-cas-dingerence-pendant-la-presidentielle.html.

Lecomte, Frederic, and Malina Charlot. 2019. “France: Cybersecurity 2020.” *ICLG.com*, accessed June 15, 2020, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france.

Lee, Sang Yeal. 2014. “When do consumers believe puffery claims? The moderating role of brand familiarity and repetition.” *Journal of Promotion Management* 20(2): 219-239.

Leukfeldt, Rutger. 2017. Research Agenda The Human Factors in Cybercrime and *Cybersecurity*. The Hague: Eleven International Publishing

Li, Xiaorong. 2010. “Google and the Cyber Infiltration.” *Philosophy and Public Policy Quarterly*, 30(1-2): 13-17.

Luiijf, H.A.M., Kim Besseling, Maartje Spoelstra, and Patrick de Graaf. 2013. “Ten National Cyber Security Strategies: A Comparison.” Conference Paper TNO The Hague, Netherlands.

Maloney, Sarah. 2018. “What is an Advanced Persistent Threat (APT)?” *Cybereason.com,* accessed May 30, 2020, https://www.cybereason.com/blog/advanced-persistent-threat-apt.

Maras, Marie-Helen. 2016. *Cybercriminology.* Oxford, UK: Oxford University Press.

Marwick, Alice and Rebecca Lewis. 2017. “Media Manipulation and Disinformation Online.” *Data and Society Research Institute* 1-106.

Masters, Jonathan. 2018. “Russia, Trump, and the 2016 U.S. Election.” *Council on Foreign Relations,* accessed May 4th, 2020, https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

Matishak, Martin. 2018. “What we know about Russia’s election hacking.” *Politico.eu,* accessed May 5th, 2020, https://www.politico.eu/article/russia-hacking-us-election-what-we-know/.

Mediapool. 2019a. “Властите засега знаят само, че НАП е хакната от чужбина, без да разбере.” *Mediapool.bg,* accessed June 4, 2020, https://www.mediapool.bg/vlastite-zasega-znayat-samo-che-nap-e-haknata-ot-chuzhbina-bez-da-razbere-news295719.html.

Mediapool. 2019b. “НАП е глобена с 5.1 млн. лв. заради теча на лични данни.” *Mediapool.bg,* accessed May 20, 2020, https://www.mediapool.bg/nap-e-globena-s-51-mln-lv-zaradi-techa-na-lichni-danni-news297373.html.

Ministère de l’Europe et des Affaires Étrangères. 2017. “Stratégie internationale de la France pour le numérique.” Aix-en-Provence: Ministère de l’Europe et des Affaires Étrangères.

Ministère de l’Europe et des Affaires Étrangères. 2019. “France Diplomacy: France and Cyber security.” *Diplomatie.gouv.fr,* accessed June 11, 2020, https://www.diplomatie.gouv.fr/

en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/.

Moore, Martin. 2018. *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age.* London, UK: Oneworld Publications.

Nap.bg. 2019. "Frequently Asked Questions." *Nap.bg*, accessed June 4, 2020, https://nap.bg/en/document?id=418.

NCCIC and FBI. 2016. "GRIZZLY STEPPE – Russian Malicious Cyber Activity." *Joint Analysis Report TLP: WHITE*, JAR-16-20296A.

NCTV. N.d. "Grootste dreiging is spionage, verstoring en sabotage vanuit statelijke actoren." *NCTV.nl*, accessed May 17, 2020, https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/dreiging.

Netzpolitik. 2015. "Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure Bundestag." *Netzpolitik.org*, accessed March 29, 2020, https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/.

Neuman, Scott. 2018. "Russia's 'Fancy Bear' Reportedly Hacks German Government Network." *NRP.org*, accessed May 12, 2020, https://www.npr.org/sections/thetwo-way/2018/03/01/589787931/russias-fancy-bear-reportedly-hacks-german-government-networks?t=1592039412878.

Newman, Abraham, L. 2015. "What the "right to be forgotten" means for privacy in a digital age." *Science* 347(6621): 507-508.

Nidecki, Tomasz Andrzej. 2019. "SQL Injection Compromises Entire Country." *Acunetix.com*, accessed June 4, 2020, https://www.acunetix.com/blog/web-security-zone/sql-injection-compromises-entire-country/.

Noack, Rick. 2017. "Cyberattack on French Presidential Front-runner Bears Russian 'Fingerprints,' Research Group Says." *The Washington Post*, April 25.

Nova News. 2019a. "Кой е 20-годишният хакер, обвинен за атаката срещу НАП?." *Nova.bg*, accessed May 19, 2020, https://nova.bg/news/view/2019/07/18/257264/кой-е-20-годишният-хакер-обвинен-за-атаката-срещу-нап.

Nova News. 2019b. “Ударна подкрепа за Кристиян Бойков в интернет.” *Nova.bg*, accessed May 19, 2020, https://nova.bg/news/view/2019/07/20/257492/ударна-подкрепа-за-кристиян-бойков-в-интернет.

Nova news. 2020. “НАП обжалва глобата на КЗЛД от 5,1 млн. лв. за теча на данни.” *Nova.bg*, accessed May 20, 2020, https://nova.bg/news/view/2020/02/10/277503/нап-обжалва-глобата-на-кзлд-от-51-млн-лв-за-теча-на-данни/.

Novinite. 2019. “TAD Group Owner Ivan Todorov Was Arrested at the Airport.” *Novinite.com*, accessed June 4, 2020, https://www.novinite.com/articles/198912/TAD+Group+Owner+Ivan+Todorov+Was+Arrested+at+the+Airport.

Oh, Sangkyo and Kyungho Lee. 2014. “The need for specific penalties for hacking in Criminal law.” *The Scientific World Journal* 1-7.

Omand, David. 2018. “The threats from modern digital subversion and sedition.” *Journal of Cyber Policy* 3(1): 5-23.

Ouest France. 2017. “Fuite de documents En Marche: les hackers ont trouvé la faille.” *Ouest France*, May 6.

Pancheva, Stoeva Desislava. 2017. “Challenges to building critical infrastructure policies in a complicated cyber environment.” *Globalization, the State and the Individual* 2(14): 263-267.

Parlement.com. N.d. “Miljoenennota.” *Parlement.com*, accessed June 21, 2020, https://www.parlement.com/id/vh8lnhrptxwp/miljoenennota.

Portswigger. 2020. “SQL injection.” *Portswigger.net*, accessed June 4, 2020, https://portswigger.net/web-security/sql-injection.

Pozen, David, E. 2013. “The leaky Leviathan: Why the government condemns and condones unlawful disclosures or information.” *Harvard Law Review* 127(2): 512-635.

President of the Republic of Bulgaria. 2012. “Consultative Council for National Security.” *M.president.bg*, accessed May 21, 2020, https://m.president.bg/en/cat70/Consultative-Council-for-National-Security.

Privacy Shield. N.d. “Bulgaria – Safety and Security.” *Privacyshield.gov*, accessed May 20, 2020, https://www.privacyshield.gov/article?id=Bulgaria-Safety-and-Security.

Protrka, Nikola, Kristijan Maric and Michael Plecas. 2017. “Challenges and aspects of cyber security in the republic of croatia.” *Acta Economica et Turistica* 3(1): 87-95.

Rafailovich, Julia. 2019. “Palken Georgiev appointed consul to Valencia but Bulgarian citizens launch a petition against, TAD Group parent company to sue Bulgaria for reputation damage.” *Mediapool.bg*, accessed Jun 4, 2020, https://www.mediapool.bg/plamen-georgiev-appointed-consul-to-valencia-but-bulgarian-citizens-launch-a-petition-against-tad-group-parent-company-to-sue--news296989.html.

Ramadani, Suci, Andysah Putera Utama Siahaan, Sutrisno, Syafruddin Ritonga, Wan Rizca Amelia, Hasbiana Dalimunthe and Riswan Munthe. 2019. “Impact of Cybercrime on Technological and Financial Developments.” *International Journal for Innovative Research in Multidisciplinary Field* 4(10): 341-344.

Raulin, Nathalie and Guillaume Gendron. 2017. “Piratage: l’équipe Macron sur le pont.” *Libération*, accessed March 29, 2020, https://www.liberation.fr/france/2017/08/10/piratage-l-equipe-macron-sur-le-pont_1589281.

Reuters, Markus. 2019. “Doxing: der kampf um datasicherheit wird au funderen computern entschieden.” *Netzpolitik.com,* accessed May 16, 2020, https://netzpolitik.org/2019/doxing-doxing-der-kampf-um-datensicherheit-wird-auf-unseren-computern-entschieden/.

Rose, Michel and Denis Dyomkin. 2017. “After talks, France’s Macron hits out at Russian media, Putin denies hacking.” *Reuters*, May 29, accessed March 25, 2020, https://www.reuters.com /article/us-france-russia-idUSKBN18P030.

Saeed, Saim. 2017. “German AfD leader loses case against TV show that called her ‘Nazi slut’.” *Politico,* May 17, accessed March 29, 2020, https://www.politico.eu/article/german-afd-leader-loses-case-against-tv-show-that-called-her-nazi-slut/.

Santora, Marc. 2019. “5 Million Bulgarians Have Their Personal Data Stolen in Hack.” *The New York Times,* July 17.

Santora, March and Eric Schmitt. 2019. “Russia suspect by some in giant Bulgaria hack.” *The New York Times,* August 14.

Schaake, Marietje. 2019. “Germany’s data hack is a wake-up call to Europe.” *Financial Times,* January 16.

Schallbruch, Martin and Isabel Skierka. 2018. *Cybersecurity in Germany*. Berlin: Springer.

Schneier, Bruce. N.d. “Cyberconflicts and National Security.” *UN Chronicle,* accessed June 10, 2020, https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security.

Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN). 2015. “French National Digital Security Strategy.” Paris: SGDSN.

Shalal, Andrea and Petra Jasper. 2017. “Germany needs tougher laws against cyber crime, top policeman tells paper.” *Reuters,* August 5, accessed March 29, 2020, https://www.reuters.com/article/us-germany-crime-cyber/germany-needs-tougher-laws-against-cyber-crime-top-policeman-tells-paper-idUSKBN1AL09C.

Sheridan, Kelly. 2019. “The Ripple Effect of Data Breaches: How Damage Spread.” *DarkReading.com,* accessed April 25, 2020, https://www.darkreading.com/threat-intelligence/the-ripple-effect-of-data-breaches-how-damage-spreads/d/d-id/1336351.

Shires, James. 2019. “Hack-and-leak operations: intrusion and influence in the Gulf.” *Journal of Cyber Policy* 4(2): 235-256.

Simonski, Krasimir, and Dr. George Sharkov. 2016. “National Cyber Security Strategy Cyber Resilient Bulgaria 2020.” *Regional Cybersecurity Forum* and *ITU.int,* accessed May 29, 2020, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf

Skurnik, Ian, Carolyn Yoon, Denise C. Parc and Norbert Schwartz. 2005. “How warnings about false claims become recommendations.” *Journal of Consumer Research* 31(4): 713-724.

Sorrell, Tom. 2015. “Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous.” *Journal of Human Rights Practice* 7(3): 391-410.

Sputnik. 2017. “Ex-French Economy Minister Macron Could be ‘US Agent’ Lobbying Banks’ Interests.” *SputnikNews.com,* accessed March 29, 2020, https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/.

State e-Government Agency. 2020. “МЕТОДИКА И ПРАВИЛА ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА ЗА СЪОТВЕТСТВИЕ С МЕРКИТЕ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, ОПРЕДЕЛЕНИ С НАРЕДБАТА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ.” Sofia: Republic of Bulgaria – State e-Government Agency.

Stoltenberg, Jens. 2019. “NATO will defend itself.” *Prospect’s New Cyber Resilience Supplement*, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.

Stoyanov, Mikhail. 2019. “Приходната агенция обмисля да заведе дело срещу "ТАД груп", за да изкара пари за глобата си.” *Devnik.bg*, accessed June 6, 2020, https://www.dnevnik.bg/bulgaria/2019/08/29/3956556_prihodnata_agenciia_obmislia_da_zavede_delo_sreshtu/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhiyx68DvQGPNUqYP-0LpyGA0eYBzw/.

Stoyanova, Petya. 2019. “КЗЛД: Сериозни пропуски в работата на НАП са причина за теча на лични данни.” *Investor.bg*, accessed May 20, 2020, https://www.investor.bg/ikonomika-i-politika/332/a/kzld-seriozni-propuski-v-rabotata-na-nap-sa-prichina-za-techa-na-lichni-danni-288793/.

Tambini, Damian. 2017. “Study on the use of internet in electoral campaigns.” *Council of Europe Study DGI* 11: 1-30.

Taylor, Paul, A. 1999. Hackers: Crime in the digital sublime. London, UK: Routledge

Thevior, Anaïs. 2013. “Un silence numérique bavard. Controverses autour de l’interdiction de la propaganda politique en ligne avant le vote.” *Mots* 103: 55-70.

Tiede, P., J. Röpcke, E. Piatov and F. Solms-Lauback. 2019. “Behörden wussten schon im Dezember von Hacker-Angriff.” *Bild*, January 4, accessed March 29, 2020, https://www.bild.de/politik/inland/politik-inland/hacker-angriff-daten-von-politikern-gestohlen-und-veroeffentlicht-59349480.bild.html#fromWall.

Tonchev, Boris. 2019. “Прокуратурата повдигна обвинения срещу Кристиян Бойков и неговите шефове копирано.” *Debati.bg*, accessed May 19, 2020, https://debati.bg/prokuraturata-povdigna-obvinenia-sreshtu-kristian-boykov-i-negovite-shefove/.

Transparency International. 2020. “Corruption Perception Index 2019.” Berlin: Transparency international.

Trimborn, Marion. 2017. “Hacker im Staatsauftrag: Was haben unbescholtene Bürger zu befürchten?” *Neue Osnabrücker Zeitung*, September 14.

Tsohou, Aggeliki, Maria Karyda and Spyron Kokalakis. 2015. “Analyzing the role of cognitive and cultural biases in the internationalization of information security policies: Recommendations for information security awareness programs.” *Computers & Security* 52: 128-141.

Untersinger, Martin. 2017. “Cyberattaques: la France menace de “mesures de rétorision” tour Etat qui interférerait dans l’élection.” *Le Monde*, February 15.

Velikova, Silvia. 2020a. “Съдът отложи за 11 май делото за хакерската атака срещу НАП.”*BNR.bg*, February 10.

Velikova, Silvia. 2020b. “Задържаният за хакерската атака срещу НАП Иван Тодоров вече е на свобода.” *BNR.bg*, February 27.

Vilmer, Jean-Baptiste, Jeangène, Alexandre Escorcia, Marine Guillaume and Janaina Gerrera. 2018. “Information Manipulation: A challenge for our Democracies.” Report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris.

Vilmer, Jean-Baptiste, Jeangène. 2019. “The “Macron Leaks” Operation: A post-Mortem.” *Atlantic Council* 1-58.

Volkskrant, de. 2019. “Student (20) zat achter hack van honderden Duitse politici.” De Volkskrant, January 8.

WikiLeaks. 2015. “What is WikiLeaks.” *Wikileaks.org*, accessed May 14, 2020, https://wikileaks.org/What-is-WikiLeaks.html.

WikiLeaks. N.d. “Macron Campaign Emails.” *Wikileaks.org*, accessed June 6, 2020, https://wikileaks.org/macron-emails/.

Willsher, Kim and Jon Henley. 2017. “Emmanuel Macron’s campaign hacked on eve of French election.” *The Guardian*, May 6.

Ziel, Arjen, van der. 2019. “Benoeming naziburgemeester schokt Duitsland.” *Trouw*, September 9.

Zook, Mattew and Mark Graham. 2017. “Hacking code/space: Confounding the code of global capitalism.” *Transactions of the Institute of British Geographers* 43(3): 390-404.