The 2007 Cyberattacks in Estonia: A quantitative analysis of the impact of cyberattacks on public support

Nes, Demi van de

The 2007 Cyberattacks in Estonia: A quantitative analysis of the impact of cyberattacks on public support

Demi van de Nes

Public Administration: Economics and Governance

Sarah Giest
06-01-2022
15127 words

Abstract

State-sponsored cyberattacks are increasing. Although most attacks have a motivation like espionage, theft, and sabotage, there are also attacks motived to disrupt or interfere with a country to negatively affect public support for the incumbent government. Even though there are plenty of examples of cyberattacks with these motivations, the actual effect of public support towards the government has not been analyzed yet. According to the rally-around-the-flag theory, sudden, international and short events such as state-sponsored cyberattack should increase public support for government instead of decrease, as the aim of the attack. In this paper, a regression discontinuity analysis is conducted on the 2007 Estonian cyberattacks. Thereby, the satisfaction levels with the government and democracy are measured before and during the attack. The effect of cyberattacks on both the satisfaction with the government as well as democracy are non-significant. In other words, state-sponsored cyberattacks do not affect the population's support for government. This is remarkable because it directly contradicts the purpose of the attack. It raises the follow-up question to what extent these types of attacks are effective.

Index

Introduction

One of the greatest threats in this day and age are cyberattacks. State-sponsored cyberattacks are increasing (General Intelligence and Security Service, 2021; Osawa, 2017). There are numerous examples of recent cyberattacks. In 2020, Iranian hackers attacked the WHO COVID-19 department, the Chinese government was accused of stealing U.S. research on a COVID vaccine, and Russian government-associated hackers attacked Germany's power companies (Center for Strategic and International Studies, 2022). In 2021, North Korea started cyber espionage missions, the EU was hit by cyberattacks of an unknown origin, and Polish political officials fell victim to an email attack originating from Russia (Center for Strategic and International Studies, 2022). In 2022, examples of cyberattacks are Chinese government-associated hackers attacking US government agencies, Israeli government websites being offline due to DDoS attacks, and Russian-linked hackers attacking the Lithuanian national energy provider (Center for Strategic and International Studies, 2022). These attacks are only the tip of the iceberg.

State-sponsored cyberattacks are on the rise (General Intelligence and Security Service, 2021; Osawa, 2017). The motivations for states to engage in cyberattacks are endless, such as cyber sabotage, espionage, intrusion, and theft (Osawa, 2017, Hunter et al., 2021). All these attacks have financial consequences, but also societal consequences, such as public support. This latter subject is often overlooked in academic research. Previous research has largely focused on the technological and financial impacts of cyber-attacks, often attacks with a more private sector focus whilst the societal effects are often left out of sight (Chapman et al., 2011; Akoto, 2021; Agrafiotis et al., 2018; Musman et al., 2011). Furthermore, there is research on public support in the light of terrorist attacks, (civil) war and natural disasters (Katz & Levin, 2015; Chowanietz, 2010; De Juan & Pierskalla, 2014; Valentino et al., 2004). Yet again, state-sponsored cyberattacks are often overlooked. Together, these two missing pieces in the academic research are a gap in the literature.

However, since daily activities, and governments, are more and more depending on the online world and state-sponsored cyberattacks are increasing, the societal consequences of state-sponsored cyberattacks are increasingly important (Saleous et al., 2022). Especially since cyberattacks are used to engage in political and societal affairs, for example, the Russian interference in multiple electoral processes such as the US elections in 2016 and several

European elections (e.g. Sweden, the Netherlands, and France) (Abrams, 2019; Reuters, 2022; Lis, 2020; Ellehuus, 2020; Brattberg & Maurer, 2018). These examples raise the question of to what extent cyberattacks on states impact the public support among the population. With this question, this thesis focuses on both state-sponsored cyberattacks and the societal consequences of these. Thereby, this thesis aims to fill the gap in the academic literature and contribute to both the societal and academic relevance of this subject.

To answer the research question, '*To what extent impact state-sponsored cyberattacks on states public support among the population?'*, this paper dives into the 2007 Cyberattacks in Estonia. During these attacks, the Estonian government, parliament, media outlets, and banking sector were hit by on-and-off DDoS attacks for 22 days (Pamment et al., 2019). Although only one Estonian citizen was convicted for the attack, there are accusations towards the involvement of the Russian government. Therefore, the 2007 Cyberattacks on Estonia are considered the first act of cyberwar (Pamment et al., 2019). Furthermore, these attacks opened the eyes of both the EU and NATO, which, in consequence, developed their cybersecurity doctrine (Juurvee & Mattiisen, 2020; Kozlowski, 2014). As there was minor (financial) damage faced by the Estonians, while the attacks lasted almost a month, the cyberattacks must have had a societal or political motivation (Tuohy, 2010). Thus, these 2007 Cyberattacks are a good case to examine the impact on public support among Estonians.

The rally-around-the-flag theory is used to analyze the impact of cyberattacks. This theory argues that a certain event might impact the incumbent governments' public support significantly. These events should be internationally orientated, affect the government directly, and be sharply focused (Mueller, 1970). If applicable to these characteristics, an event can be called a rally event. The underlying mechanism of these events is that they evoke a call for security and anger among the population. When experiencing a rally event, the citizens turn towards their government the ask for security (Bækgaard, et al., 2020; Lambert, et al., 2010). Likewise, the urgency of the event overrules the importance of other affairs and thereby comes to the fore (Bækgaard, et al., 2020; Lambert, et al., 2010). Moreover, it incites anger among the population toward their attacker (Lambert, et al., 2011). These three emotional reactions towards a rally event generate higher support levels for the incumbent government.

To apply the rally-around-the-flag theory to the 2007 Cyberattacks in Estonia, the European Social Survey is used. This survey provides a unique opportunity to measure the satisfaction

ratings before and during cyberattacks. A regression discontinuity design is used to analyze the impact of the attack on the satisfaction ratings of the Estonians. The start of the attack is used as the clean-on-and-off switch. The results presented an interesting pattern whereby in the first month of the attack satisfaction ratings rose to a peak. In the second month of the attack, these ratings dropped again to near the ratings before the attack. Nonetheless, the results also demonstrated that the 2007 Cyberattacks had no significant effect on the satisfaction ratings of Estonians on their government or democracy. These results indicate that using cyberattacks as a means to disrupt or tarnish public support in a country might not be successful.

This paper will proceed as follows. Section 1 dives into the literature review and the theoretical framework of this paper. Section 2 discusses the methodology and data. Section 3 explains the case of the 2007 Cyberattacks in Estonia, and section 4 analyses the presented results. Finally, section 5 concludes the paper.

1. Theoretical framework

To understand the relationship between cyberattacks and public support, this section drives into the theory and links both concepts to each other. The theory of public support and event theory is varied. However, in this paper, the focus is on the positive effect of rally events on public support. On the contrary, it could be argued that public support is harmed by an event such as cyberattacks. This theoretical background allows to form hypotheses.

1.1 Public support

According to the democratic accountability theory, there is a relationship of accountability between the incumbent leader and the population. This relationship may impact the population's public support for the incumbent (Asamoah, 2018). During rally events, this dependency relationship is challenged. According to the rally-around-the-flag theory, negative rally events increase the support of the incumbent (Mueller, 1970).

1.1.1 Public support and democratic accountability

The democratic accountability theory states that there is a dependency relationship between the government and the population. Olsen (2016) argues that democratic accountability "implies governance based on feedback, learning from experience, and the informed consent of the governed" (p. 1). This definition implies an accountable relationship between the incumbent and the population. According to the definition of Fearon (1999) accountability entails that "there is an understanding that A is obliged to act in some way on behalf of B" (p. 55) and "B is empowered by some formal institutional or perhaps informal rules to sanction or reward A for her activities or performance in this capacity" (p. 55). Thus, this accountability relationship has consequences. When an incumbent complies with the population's expectations, the incumbent could be rewarded with public support. Likewise, when an incumbent acts against the population's expectations, the incumbent could be punished with decreasing public support (Ferejohn, 1986; Asamoah, 2018). That being the case, public support is important as it offers the incumbent legitimacy (Lagos, 2003). This public support may be reflected in elections with re-election (Fearon, 1999; Manin, et al., 1999). However, in non-election times, this may not be directly measurable in election outcomes. Therefore, other forms of public support could be exposed like direct feedback and learning from the past (Olsen, 2016). As the support of the public could impact the incumbent's future, the incumbent is likely to adapt to the public's

interests (Ferejohn, 1986; Asamoah, 2018). In short, there is an ongoing process of accountability between the incumbent and the population, which impacts public support.

1.1.2 Public support and rally events

The democratic accountability theory argues that the performance of the incumbent perceived by the population could increase or decrease public support levels. Incumbent performance could be impacted during (national) events, such as terrorist attacks, natural disasters, and war. The public's evaluations of the incumbent's actions during such events could impact public support (Chanley, et al., 2000). Nonetheless, the levels of public support or a government could also be impacted by the event itself. This is called a rally-around-the-flag effect (Mueller, 1970; Nielsen & Lindvall, 2021).

The rally around the flag effect occurs when a country turns into a crisis. According to Mueller (1970), these crises are so-called 'rally points'. These rally points occur when three conditions are met: I) the event has an international focus; II) the event should involve the country directly and therefore be relevant to the citizens; and III) the event should be short-term focused to keep the attention of the population (Mueller, 1970). Events like rally events often have positive effects on the support of incumbents (Mueller, 1970; Nielsen & Lindvall, 2021). There are several psychological assumptions arguing why the population increases their support for incumbents during these rally points. The first one is 'security' assuming that the crisis creates fear among the population. Therefore, they turn toward the incumbent or government to seek protection and security. Moreover, crises overrule other political concerns. The rally point makes political indifferences less important and creates a single focus on the current crisis. This might lift the ratings for the incumbent, as previous malfunctions are pushed to the background (Bækgaard, et al., 2020; Lambert, et al., 2011; Lambert, et al., 2010). Another explanation is 'anger', which assumes that negative rally events, such as attacks and war, have a greater effect on incumbent support than positive rally events, such as military victories. Negative rally events enforce emotions of anger among the population. These emotions turn the population toward their government for acting against the attacker (Lambert, et al., 2011). The effect of negative rally events on the support of the incumbent government is visible in various research (Blais, et al., 2020; Nielsen & Lindvall, 2021).

1.1.3 Conceptualization of public support

As mentioned, public support comes in various forms, such as re-election ratings, but also in direct feedback and past-learning processes (Olsen, 2016). Consequently, in research, public support is difficult to measure during non-election times. Therefore, public satisfaction is often used as a substitute for public support (Lagos, 2003). Although satisfaction and support are slightly different, they are often used interchangeably. Whereas public support provides the legitimacy of the incumbent, public satisfaction focuses on the evaluation of the incumbent. Thus, satisfaction ratings are necessary to measure the final public support ratings. This makes satisfaction an important indicator of public support. They are two sides of the same coin (Lagos, 2003). Another substitute for measuring public support is satisfaction with democracy (McAllister & White, 2004; Zmerli & Newton, 2008; Stecker & Tausendpfund, 2016). According to McAllister and White (2014), people's satisfaction with democracy correlates with their support for the incumbent. When the public has a positive assessment of democracy, it is more likely to support the incumbent government because it was justified in taking office (McAllister & White, 2014).

1.1.4 Public support among subgroups

The above-mentioned indicators (satisfaction with government and satisfaction with democracy) are beneficial when measuring public support in non-election times. However, public support does not develop equally among all groups. Crow (2010) argues that "personal resources" (p. 52) could play a part in whether someone is satisfied with the state of the democracy or their incumbent. One of these characteristics is gender. Overall, women tend to have a more neutral opinion regarding democracy than men. In research on political attitudes in Africa, women indicated that they were less satisfied with the current democracy, but more neutral towards the state of the democracy compared to men (Logan & Bratton, 2006). Similar results are seen in national research on attitudes towards democracy and government in Europe and Mexico: women are less satisfied than men (Hansen & Goenaga, 2019; Crow, 2010).

A second characteristic that could impact satisfaction levels is age. In Australia, the baby boomer generation tends to be more satisfied with the democracy than younger generations (Stoker et al., 2018). Stoker et al. (2018) find an interesting movement in the satisfaction ratings among the older generations in Australia. On the one hand, they contain the most dissatisfied individuals, but on the other hand, they also include the most satisfied individuals. Contrary to younger generations, the elder generation is less neutral regarding their satisfaction with

democracy and tends to take a stand (Stoker et al., 2018). Crow (2010) argues that the difference in satisfaction levels between the older and the younger generations results from their historical awareness. In many parts of the world, the current elderly experienced in more direct or indirect ways the consequences of non-democratic regimes. These memories make them more satisfied with the current political situation (Crow, 2010). Furthermore, older citizens often have more stability and a higher income, which makes them less vulnerable to political failures (Crow, 2010).

Third, the levels of education impact citizens' satisfaction (Crow, 2010; Almond & Verba, 2015; Wang, 2005). In research on China and Taiwan, higher educational levels are correlated with lower government satisfaction (Huang, 2018). Similar results are visible in Wang's research (2005) on satisfaction with democracy and incumbents. Both indicators were negatively correlated with higher educational levels. Wang (2005) argues that the underlying mechanism of this relationship is that higher-educated citizens are more critical of their government. This argument is strengthened by Almond and Verba (2015) stating that higher educational levels go hand in hand with higher political interests and awareness, nationally and internationally. These increased levels of political interests may impact the citizens' critical attitude towards the incumbent and democracy.

The final personal characteristic that affects satisfaction is belonging to an ethnic minority. In research on the democratic satisfaction of ethnic minorities in the United Kingdom, citizens belonging to an ethnic minority were more satisfied with democracy than their majority counterparts (Sanders et al., 2013). However, in several studies of Nigeria, Estonia, and Latvia, ethnic minorities' democratic satisfaction is lower than that of the majority group (Inglehart & Carballo, 1997; Chereson & Estes, 2022). This difference can be explained by the fact that democratic satisfaction is influenced by the extent to which citizens belonging to ethnic minorities have a psychological bond with politics in their country. When this bond is stronger, their democratic satisfaction will also be higher, and vice versa (Inglehart & Carballo, 1997; Sanders et al., 2013). Furthermore, Inglehart and Carballo (1997) argue that "historical grievances" (p. 25) between ethnic groups may also play a role. When there are many (historical) tensions between minority and majority groups, the satisfaction of the former will also be lower (Inglehart & Carballo, 1997). Thus, it is impossible to say whether citizens belonging to ethnic minorities have higher or lower satisfaction scores. These scores vary from country to country and from ethnic minority to ethnic minority.

In short, according to the democratic accountability theory, public support is impacted by the performance of the government as perceived by the population. When a rally event occurs, these performances are positively strengthened by rally event effects. Due to increased feelings of fear and anger among the population, public support levels increase. While public support ratings differ per subgroup, the overall ratings increase and the incumbent is perceived more positively. This leads to the first hypothesis:

I. A cyberattack has a positive effect on public support towards the government, ceteris paribus.

1.2 Cyberattacks

This paper analyzes the effect of cyberattacks on the population's public support concerning the government. Cyberattacks conducted by states often articulate a certain political position, and therefore, often have political incentives. Effects of such cyberattacks are, amongst others, impacting the perception of the public towards their government. Previous research has shown that cyberattacks have negative societal effects.

Information and Communications Technology (ICT) has an increasing role in daily lives (Van den Berg, et al., 2015a). Activities are increasingly online, especially since the latest pandemic which forced millions to work from home (Saleous et al., 2022). However, not just daily activities moved from the offline world to the online world. More fundamental societal functions also moved to the online world, such as banking, managing infrastructure, government activities, and even, in some countries, democratic participation as voting. All these online activities are cyber activities, which are taking place in cyberspace (Van den Berg, 2015b). This cyberspace needs to be protected, as cyber activities could fall victim to types of cybercrimes.

1.2.1 Cybersecurity as a public good

The protection of this cyberspace is called cybersecurity, or "the absence of danger or damage caused by disruption or failure of ICT, or by abuse of ICT" (Van den Berg, 2015b, p. 4). Cybersecurity could be seen as a public good. In economic theory, public goods are goods that are both non-excludable and non-rivalrous (Stevens, et al., 2017, Chapter 12.5; Kianpour, et al., 2022; Rosenzweig, 2011). I.e., one cannot enjoy these goods without preventing others from enjoying them as well (non-excludable). Moreover, the consumption of public goods does

not diminish the availability for others (non-rivalrous) (Stevens, et al., 2017; Mulligan & Schneider, 2011). This type of goods could be differentiated from other types of goods: private goods, club goods, and common goods (see figure 1) (Kianpour, et al., 2022; Rosenzweig, 2011).

	Rivalrous ***(Use by A does affect use by B)***	**Non-rivalrous** ***(Use by A does not affect use by B)***
Excludable ***(Use by A prevents use by B)***	Private goods *Cars, apples*	Club goods *Museum, cable television network*
Non-excludable ***(Use by A does not prevent use by B)***	Common goods *Oil wells, national forests*	Public goods *National defense, country's financial stability*

Figure 1. Typology of economic goods (Kianpour, et al., 2022, p. 3; Rosenzweig, 2011)

The two characteristics of public goods apply to *public* cybersecurity (Mulligan & Schneider, 2011; Kianpour, et al., 2022). Non-rivalrous apply to *public* cybersecurity as the system's protection of one individual's data does not diminish the security of another's data protection. *Public* cybersecurity is non-excludable as individuals cannot be excluded from the benefits of *public* cybersecurity (Mulligan & Schneider, 2011). The consequence of assuming that cybersecurity is a public good is that it creates a social dilemma (Stevens, et al., 2017). People cannot be excluded from these types of goods, even if they do not (financially) contribute to them. Everyone will enjoy the benefits of public cybersecurity regardless of their contributions. This makes it difficult for markets to provide goods that are both non-excludable and non-rivalrous (Stevens, et al., 2017).

The non-rival and non-excludable aspects of public goods lead to two types of market failures (Stevens, et al., 2017). When goods are non-rivalrous, the corresponding marginal costs are zero (Stevens, et al., 2017). Providers of goods aim for a Pareto-efficient situation where the sum of the consumer and producer surplus is maximized (Bowles, et al., 2017). Or, in other words, the costs of producing one extra unit (marginal costs) should be equal to the price (Stevens, et al., 2017). However, when producing a public good such as cybersecurity, the marginal costs are zero as it does not affect one's ability to use the product. The occurring problem is that to be Pareto-efficient, one cannot be better off without someone else being worse off, and the marginal costs should be equal to the set price (Bowles, et al., 2017). Therefore, when the marginal costs are zero, the price should be zero as well. This makes it difficult for a market to provide non-rivalrous goods (Stevens, et al., 2017). As mentioned, non-excludable goods make it difficult, if not impossible, to exclude people from using them,

even if they do not (financially) contribute to the good (Stevens, et al., 2017). Together, the marginal costs being equal to zero and the unpriceability of the goods makes it impossible for the markets to allocate public cybersecurity (Mulligan & Schneider, 2011). Therefore, public cybersecurity should be provided by the government.

1.2.2 Conceptualization of cyberattacks

Thus, the aim of cybersecurity is to protect the cyberspace from cyberattacks, such as disruption, failure, or abuse (Van den Berg, 2015b). These threats can occur by accident but also on purpose. When cybersecurity is threatened, cyber activities are threatened as well (Van den Berg, 2015b). Events like disruption, failure, or abuse of ICT fit into the Tallinn Manual 2.0 definition of cyberattacks: "A cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt, 2016, p. 1000). The problem with this, and many other definitions regarding cyberattacks, is that these are broad and ambiguous (Kadivar, 2014). By analyzing common definitions of cyberattacks, Kadivar (2014) distinguished five attributes that are connected to the main concept:

1. Actors: according to Kadivar (2014) in each cyberattack, there are at least two actors: the attacker and the attacked. The executive actor could be any kind of person or organization, e.g., either state actors or non-state actors with each their motives (Kadivar, 2014; Blank, 2013; Brantly, 2014). Similarly, the attacked actors could also be state and non-state actors (Dinicu, 2014). However, it is important to note that cyber-attacks are often asymmetric attacks, meaning that there is a level of disparity between those who execute the attack and those who receive the attack (Dinicu, 2014).
2. Assets: the targeted assets may vary by the different attacks and are as varied as the actors involved (Kadivar, 2014). For example, actors could tempt to attack the states or organizational infrastructure but also target individual accounts (Li & Liu, 2021; Kadivar, 2014).
3. Motivations: as mentioned above, the underlying motivation varies by situation and actor (Kadivar, 2014; Blank, 2013; Brantly, 2014). Examples of these motivations are controlling the targeted asset, stealing money or data from the asset, preventing the asset from executing its tasks, and gaining access to other devices or systems (Lu & Reeves, 2014; Kadivar, 2014).
4. Effects: effects of executed attacks vary per situation (figure 2) (Kadivar, 2014; Agrafiotis, et al., 2018). Agrafiotis et al. (2018) distinguish five types of harm that could

result from cyberattacks: I) digital harm, e.g., theft and leaks; II) economic harm, e.g., fall in stock prices and economic disruptions; III) psychological harm, e.g., experiencing anxiety or embarrassment; IV) reputational harm, e.g., damaged relationships; and V) societal harm, e.g., negative effects on the public perceptions (Agrafiotis, et al., 2018). Not all of the above effects apply to every cyberattack. For example, individuals will be more likely to face psychological harm than governments. Similarly, individuals will be less likely to experience societal harm than governments (Agrafiotis, et al., 2018)

5. Duration of the attack (Kadivar, 2014).

1.2.3 Cyberattacks against states

As mentioned, there is a vast variety of types of cyberattacks, depending on the actors involved, the targeted assets, the underlying motivation, the harm done, and the duration of the attack (Kadivar, 2014). This paper involves cyberattacks against states. Cyberattacks against state actors have increased over the last few years (Bendovschi, 2015). These types of attacks are challenging, as they threaten the entire infrastructure of nations (Dinicu, 2014). According to Lewis (2010), contemporary states face broadly four types of threats, coming from cyberspace: I) Economic espionage, attackers aiming to steal confidential economic information and intellectual property; II) Political and military espionage, attackers aiming to steal confidential political and military information; III) Cybercrime, attackers are financially motivated and therefore aim to steal money and financial assets rather than information; and IV) Cyberwar, attackers are motivated to destroy critical infrastructure. Together, these types of attacks could pose danger to a country's security and the continuation of critical and less critical cyber activities (Dinicu, 2014).

But why do states use cyberattacks to reach their political goals? According to Nazario (2009), these attacks often express the support of governments, for example during the 2007 Russian Elections when the opposition party of Kasparov suffered DDoS attacks. I.e., the attacks articulate government positions, when executed or commissioned by governments. DDoS attacks are meant to cause damage, either politically, socially, or economically. However, it is hard to attribute attacks to actors, especially when they are not claimed by actors (Nazario, 2009). This makes cyberattacks useful tools to express or exercise government positions, without facing the consequences, as attributing attacks is difficult without substantial evidence.

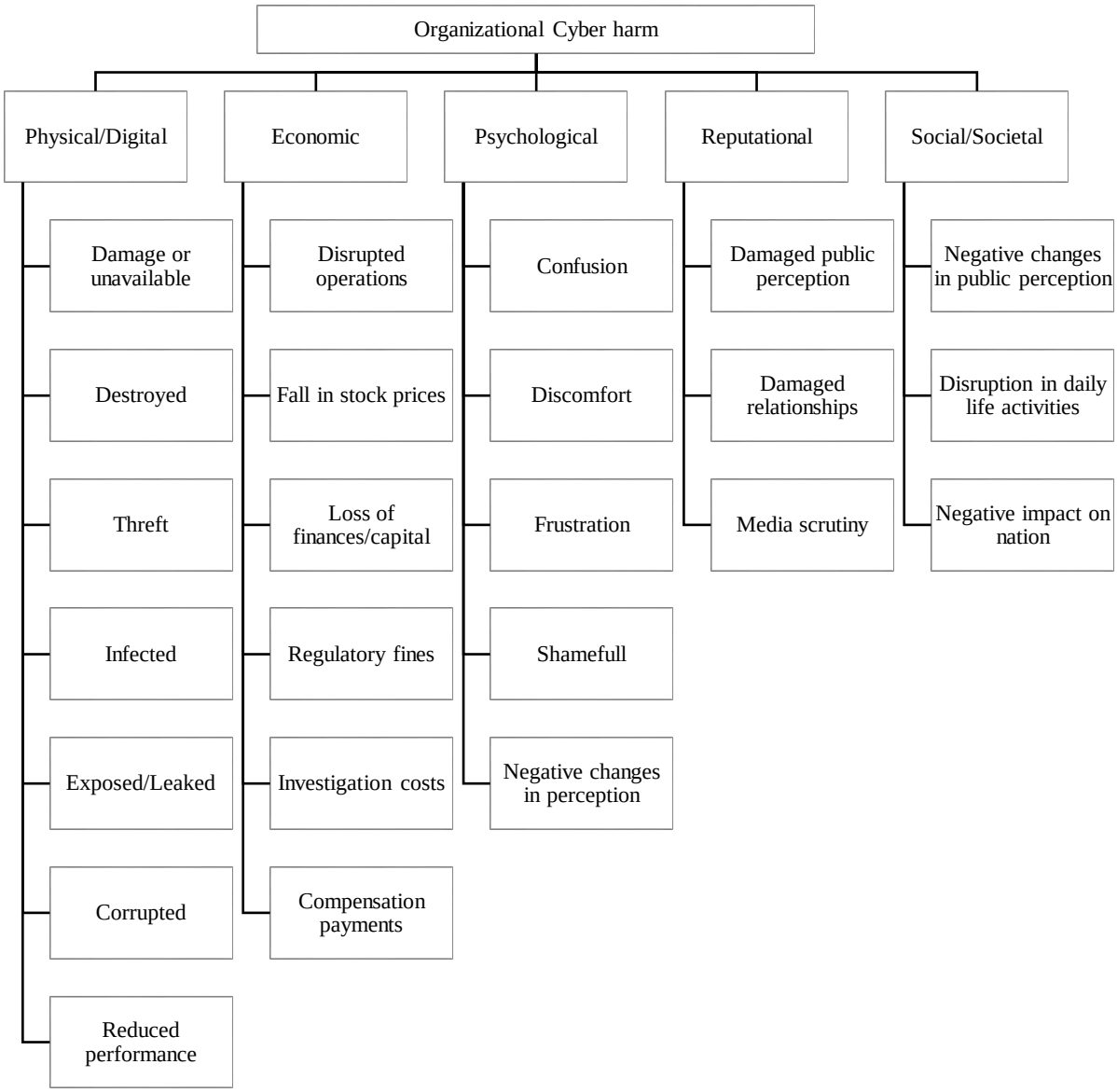


Figure 2. An adjusted form of the taxonomy of organizational cyber-harms (Agrafiotis, et al., 2018)

1.2.4 Societal effects of cyber attacks

As all cyber-attacks have different motivations and are strengthened by the problem of cybersecurity being a public good, their effects on the assets are numerous as well (Kadivar, 2014). Agrafiotis et al. (2018) took the principles of harm and applied them to cyberattacks. This resulted in a taxonomy of cyber-harm (Agrafiotis, et al., 2018). Figure 2 depicts the Agrafiotis et al. (2018) organizational cyber harm taxonomy in a compressed form. These types of harm are neither exclusive nor extensive. Organizations could face several types of cyber-harm, and types of harm could also overlap within diverse types (Agrafiotis, et al., 2018). The original taxonomy applies to harm experienced by organizations. The compressed form of the

taxonomy includes the types of harm that could be experienced by states as well. From this taxonomy, the societal effects are highlighted.

In the Agrafiotis et al. (2018) taxonomy, societal harm is experienced by organizations and results in negative public perceptions, disruptions in cyber activities, and a negative impact on the nation due to lacking services. Similar effects could be felt by states after a cyberattack. Cyberattacks may decrease public support for the incumbent government (Shandler & Gomez, 2022).

This relationship lies within the earlier discussed theory on public support and public goods. Due to market failures, the government is responsible for providing cybersecurity. Therefore, when the country faces a cyberattack, the government has failed in its task to protect its citizens and their cyber activities. When a government does not comply with public expectations, the incumbent could be punished with decreasing public support (Ferejohn, 1986; Asamoah, 2018). Thus, as the government is responsible for the country's and citizens' cybersecurity, a cyberattack could damage the public support ratings for the incumbent. The relationship between cyberattacks and diminishing public support ratings has been found in a case study on a ransomware attack in Düsseldorf. The attacks created sentiment among the public, caused by increased levels of dread, that the government was not capable of handling these types of attacks (Shandler & Gomez, 2022). In other words, the government was punished for its failure in meeting the public's expectations.

Based on the cybersecurity theory above, and the Agrafiotis et al. (2018) taxonomy, it is likely that cyberattacks might have negative societal effects. According to the taxonomy (Agrafiotis et al., 2018) cyberattacks could disrupt the daily cyber activities of the population, and cause negative changes in public support. This leads to the second hypothesis:

II. *A cyberattack has a negative effect on public support towards the government, ceteris paribus.*

2. Methodology and data

To examine the relationship between state-sponsored cyberattacks on state and the public support of the population, this paper made use of a case study on the 2007 Estonian cyberattacks in combination with the quantitative regression discontinuity approach. The quantitative analysis is explained with data from the European Social Survey, conducted in Estonia from 2006-2007. In answering the research question, this thesis distinguishes the satisfaction for the current government and that for the democracy in general to provide an as solid answer possible.

2.1 Research method

2.1.1 Case study

To study the effect of cyberattacks on public support, this paper dives into a single case study. A case study allows to single out an event and examines this apart from other ongoing events in the public sphere (Toshkov, 2016). To measure whether a cyberattack impacts the public support ratings, it is important to keep all other impact characteristics as equal as possible. A case study provides this opportunity.

There is a vast variety of types of cyberattacks, depending on the actors involved, the targeted assets, the underlying motivation, the harm down, and the duration of the attack (Kadivar, 2014). Nevertheless, this paper focuses on a specific type of cyberattacks: state-sponsored cyberattacks against other state actors. These types of attack consist of two characteristics: I) state-sponsored; and II) targeting a nation state. When cyberattacks are state-sponsored, state actors are (indirectly) involved in the attacks. State-sponsored cyberattacks are considered the most 'dangerous', as they often have the financial and technical means for executing a successful cyberattack (Dinicu, 2014). Other types of actors often lack either/both financial and/or technical assets to conduct a successful attack on a state (Dinicu, 2014). These types of attacks can be executed by all types of actors, with all types of motives and effects, such as hacktivism (politically motivated without causing serious harm) and cyberterrorism (politically motivated with causing serious harm) (Kadivar, 2014; Denning, 2001; Weimann, 2004). When state-sponsored attacks are targeting nation states, this may be called cyber warfare (Hughes & Colarik, 2017). In contrast, cyberattacks executed by non-state actors are called cybercrimes (Li & Liu, 2021). Cyber warfare attacks are often politically, economically, or military-motived cyberattacks against (the interest of) other states (Li & Liu, 2021; Kavallieros, et al., 2021).

The 2007 Cyberattacks on Estonia comply with the two characteristics mentioned above: I) state-sponsored; and II) against another nation state. Although unproven, there are strong suspicions of the involvement of the Russian government in these attacks (state-sponsored) (Herzog, 2011). Further, the attack was focused on the Estonian government (against another nation state). In fact, the attacks on Estonia are considered to be one of the first cyberwar attacks in history (Pamment et al., 2007). Moreover, it had an important impact on the cybersecurity policies of both NATO and the EU (Juurvee & Mattiisen, 2020; Kozlowski, 2014). Thus, the Estonian case had an impact on internal and external policy making. Thereby, the Estonian case is a fine case to analyze the relationship between cyberattacks and public support.

2.1.2 Regression Discontinuity

To analyze the possible relation between cyberattacks and public support, a regression discontinuity design is used. The 2007 Cyberattacks on Estonia created a clear division between the population which experienced the cyberattack (April 27th 2007, and later) and the population which had not experience the cyberattack yet (before April 27th 2007). This division between the two groups creates the opportunity to conduct a regression discontinuity analysis. As this paper works with observational data, a randomized trial is not a possibility (Angrist & Pischke, 2014). A regression discontinuity analyses assumes at the independent variable is as-good-as-random applied to the case: it is a natural experiment (Angrist & Pischke, 2014; (Sekhon & Titiunik, 2017). This assumes that the groups around the treatment are as similar as possible concerning most characteristics, except for the application of the treatment. This creates a control group (before the treatment) and a treatment group (after the treatment). In the Estonian cyberattack case, the treatment is the cyberattack. This is a clean cutoff: the population before the 2007 Cyberattacks has not been exposed to the cyberattack, while the Estonian population after the cyberattack has been exposed to the attack. As this is a clear on-and-off-switch, the assumption is that this is a sharp regression discontinuity analysis (Angrist & Pischke, 2014). The treatment can be written in as D_d, whereby $D_i = 1$ indicates that the population is exposed to the cyberattacks (treatment group) and $D_i = 0$ indicates that the population is not exposed to the cyberattacks (control group) (Angrist & Pischke, 2015). D is hereby deterministic on *i* (individual), which means that if *i* is known, the value of D_i is known as well. Using the RD method leads to the following equation:

$$\gamma_i = \alpha + \beta R_i + \rho D_i + \varepsilon_i$$

Hereby, γ_i is the outcome variable. In this thesis, public support. R_i is the running variable, i.e. the months before or after the cut-off. The corresponding beta is the causal effect of the running variable. D_i is the treatment dummy. In this paper, the treatment dummy is the presence of the cyberattack. The corresponding ρ is the treatment effect (Angrist & Pischke, 2014).

2.2 Dataset

The European Social Survey (ESS) is used to analyze the relationship between cyberattacks and public support. This type of survey is a cross-national European survey, focusing on the attitudes of Europeans. The European Social Survey has been conducted since 2001, and currently has 10 rounds up to 2020 (European Social Survey, n.d.-a). The ESS used a systematic random sampling method by implicit stratification. In Estonia, individuals of at least 15 years old were randomly selected from data provided by the Estonian Ministry of Internal Affairs (European Social Survey, n.d.-b).

In the RD analysis, ESS round 3[1] is used, which includes 1515 cases and has been conducted from October 25th, 2006, up to May 21st, 2007.[2] The focus of the analysis is on the cyberattack on Estonia, which is a clear cut-off. The cyberattack started at April 27th, 2007 and lasted 22 days. Therefore, the cut-off is at the 27th of April. As the ESS round 3 data is collected during the cyberattacks, it offers the unique opportunity to measure the impact of the attack on public support. Consequently, the cut-off divides the sample in two groups: I) control group: the group which was interviewed before the cyberattacks, and II) treatment group: the group which was interviewed during the cyberattacks. In total, 1466 individuals were interviewed before the cyberattack (control group) and 49 were interviewed during the cyberattack (treatment group). Although the two groups differ in size, the characteristics are relatively similar. Table 1 shows the balance test.[3] As the average of several characteristics among the two groups are relatively alike among the treatment- and control group, it can be argued that both groups are randomized. This assumption makes the final analysis as close as possible to an experiment.

[1] Free downloadable at: https://ess-search.nsd.no/en/study/964cafba-fc62-4162-af01-fa40f9f9baec
[2] For the entire dataset set-up, see appendix I
[3] For all descriptive statistics, see appendix II

	Treatment group	Control group
Paid work last 7 days (% yes)	56.2%	59.2%
Years of fulltime education	12.57	12.27
Highest level of education	3.22	3.34
Age of the respondent	44.77	45.52
Gender (% female)	59.3%	54.8%
Citizen of the country (% yes)	90.8%	77.8%
N	49	1466

Table 1. Balancing test treatment group and control group: before and after the cyberattack.
Weighted by post-stratification weights

2.3 Dependent and independent variables

The independent variable is the treatment variable, and thus, the case-study: the 2007 Cyber-attacks on Estonia. The decision of this case has been highlighted above. Furthermore, in the next section, the 2007 Cyberattacks on Estonia will be further explained.

As mentioned in the literature review, the dependent variable, public support, can be operationalized in two ways. Together, these two indicators are used to answer the main research question '*To what extent impact state-sponsored cyberattacks on states the public support among the population?*' through two hypotheses: *I) A cyberattack has a positive effect on public support towards the government, ceteris paribus;* and *II) A cyberattack has a negative effect on public support towards the government, ceteris paribus.*

The first indicator is measuring public support though the satisfaction with government (Lagos, 2003). Satisfaction ratings are often used to operationalize public support in government (Kotzian, 2010; Gabel & Hix, 2005). Whereas public support provides the legitimacy of the incumbent, public satisfaction focuses on the evaluation of the incumbent. Thus, satisfaction ratings are necessary to measure the final public support ratings (Lagos, 2003). With the European Social Survey, government satisfaction ratings could be measured with the variable **"stfgov: How satisfied with the national government"** (European Social Survey, 2018, p. 104). This variable measures the interviewee's satisfaction with its government by asking the following question: "Now thinking about the [country] government, how satisfied are you with the way it is doing its job?" (European Social Survey, 2018, p. 105). The interviewee can answer this question on a scale ranging from 0 (extremely dissatisfied) to 10 (extremely satisfied) (European Social Survey, 2018). This variable is a recurring variable which occurs in round 3 of the ESS conducted in Estonia. In the dataset comparing the groups before and

after the cyberattack, there is a mean of 4.76 (S.E. is 0.058) (table 2). The minimum value is 0 (45 times) and the maximum value is 10 (19 times).

The second way of operationalizing public support is satisfaction with democracy (Zmerli & Newton, 2008; McAllister & White, 2004). People's satisfaction with democracy correlates with their support for the incumbent. When the public has a positive assessment of democracy, it is more likely to support the incumbent government because it was justified in taking office (McAllister & White, 2004). To operationalize satisfaction with democracy, there is the variable **"stfdem: How satisfied with the way democracy works in country"** (European Social Survey, 2018, p. 105). This variable measures the population's trust in democracy and refers to the question: "And on the whole, how satisfied are you with the way democracy works in [country]?" (European Social Survey, 2018, p. 105). Again, the answering-range is from 0 (extremely dissatisfied) to 10 (extremely satisfied) (European Social Survey, 2018). The question is asked in the 3rd round in Estonia. In the dataset comparing the groups before and after the cyberattack, there is a mean of 4.89 (S.E. is 0.062) (table 2). The minimum value is 0 (57 times) and the maximum value is 10 (17 times). Including both the measurement of satisfaction with democracy and the current government allows to determine whether Estonians might be unsatisfied with their current government, but satisfied with democracy, or whether they are both (dis)satisfied with both their current government and democracy.

	Mean	**S.E.**	**Min**	**Max**	**N**
Satisfied with the current government	4.76	0.058	0	10	1402
Satisfied with democracy	4.89	0.062	0	10	1349

Table 2. Descriptive statistics of both the treatment group and control group on the dependent variables.
Weighted by post-stratification weights

2.4 Subgroups

Besides the main analysis, focused on public support via satisfaction with democracy and satisfaction with the government, a subgroup analysis is also conducted. According to the theory, some subgroups might behave differently regarding satisfaction with democracy and the government. To analyze whether their pattern is also different in the case of a cyberattack, these groups are included. Based on the literature review, four different subgroups are distinguished: I) women; II) elderly (older than 55 years); III) higher educated (at least the completion of post-secondary education); and IV) ethnic minorities (mainly Russian,

Ukrainian, and Belarussian). The aim of including these subgroups is to determine whether they follow a similar pattern as the main sample when being confronted with a cyberattack.

3. Case description

This thesis focusses on the question to what extent state-sponsored cyberattacks on states impact public support. Cyberattacks are often short-lasting events. Therefore, by singling out these events, the impact on the population could be measured. Furthermore, the aim of this research is to focus on state-sponsored cyberattacks directed at nation states. These characteristics narrow down the number of options for a case study. Eventually, in this study, it was decided to focus on the 2007 Cyberattacks on the Estonian government. These cyberattacks lasted less than a month and their effects could therefore be singled out (Pamment et al., 2019; Ottis, 2008). Moreover, the Estonian government accuses the Russian government of supporting these attacks. Although the involvement of the Russian government is not proven, the Estonians themselves argue that these attacks are state-sponsored (Herzog, 2011). As this paper measures the impact of state-sponsored cyberattacks on the public support of the population, the accusation of the Estonians towards the Russian government is enough to consider these cyberattacks as state-sponsored.

The 2007 Cyberattack on the Estonian government is considered one of the first cyberwar attacks (Pamment et al., 2019). Consequently, it impacted the European and NATO cybersecurity doctrine (Juurvee & Mattiisen, 2020; Kozlowski, 2014). Before the cyberattack, there was unrest in Estonia. The source of the turmoil had its roots in Estonian and Russian history. The direct event causing this unrest was the removal of the Bronze Soldier of Tallinn on April 26th, 2007 (Ottis, 2008; Pamment et al., 2019). This statue was a memorial statue in remembrance of the Soviet victory over Nazi Germany. The statue was planted in Tallinn by the Soviets after they included Estonia in their union (Tapon, 2018; Juurvee & Mattiisen, 2020). For ethnic Russians living in Estonia, which made up around 25 percent of the total Estonian population in 2000, the statue was a memorial for the Russians who lost their lives during WWII (Minority Rights Group, 2021; Tapon, 2018; Juurvee & Mattiisen, 2020; Kozlowski, 2014). Hence, it was also the place where Russian Estonians celebrated May 9th, the Russian Victory Day. Contrarily, for many ethnic Estonians, the statue symbolizes Soviet domination, including its related deportations (Tapon, 2018; Juurvee & Mattiisen, 2020; Kozlowski, 2014). Thus, the Bronze Soldier represented two stories of liberation and occupation. This difference in symbolization led to friction about the statue (Juurvee & Mattiisen, 2020; Ottis, 2008).

Already in 1994, it was opted to remove the memorial because of its reflection of conflicting and confronting memories. The proposal was overthrown due to the large share of ethnic Russians in Tallinn. Hence, the Bronze Soldier remained in the Estonian capital. However, the resistance remained. After several (threats of) incidents of commotion during the Russian commemoration of the statue, the Estonian authorities decided to remove the Bronze Statue (Juurvee & Mattiisen, 2020). In January 2007, the Estonian government proposed the removal of the monument. In response to the preliminary removal activities concerning the statue in April, ethnic Russians gathered around the Bronze Soldier. Consequently, the Estonian government decided to remove the statue immediately on April 26th (Juurvee & Mattiisen, 2020). The removal led to riots in the country, opposing the removal of the Bronze Soldier. Furthermore, the Russian government acted upon the Estonian decision. Months before the removal, the Russian government already commented on the situation by criticizing Estonia's way of handling the situation and referring to Estonians as Nazi sympathizers (Juurvee & Mattiisen, 2020). As the Estonian government decided to remove the Bronze Soldier, the Russian government continued this discourse. However, they also disrupted trade relations with Estonia, and the Estonian embassy in Moscow was blocked (Tapon, 2008; Juurvee & Mattiisen, 2020; Kozlowski, 2014; Ottis, 2008).

Followed by this Bronze Night, the first cyberattack on the Estonian government took place. The cyberattacks happened in two waves. The first wave started on April 27th and was considered an uncoordinated and unprofessional wave of cyberattacks. The main targets were news outlets and government websites and e-mail servers (Pamment et al., 2019). On May 4th, the second wave started, which was considered more coordinated and professional in its attacks (Pamment et al., 2019). Further, the initial list of targets was expanded to, amongst others, banking institutions. On May 9th, Russia's Victory Day, there was a peak in the attacks (Kozlowski, 2014). The nature of these events were DDoS (Distributed Denial of Service) attacks (Pamment et al., 2019; Ottis, 2008). As Estonia's government services depended heavily on the internet, these attacks disrupted Estonian cyber activities. This disruption impacted the Estonian population in their daily activities and communication with the government. According to Ottis (2008), based on this reasoning, the cyberattacks were a threat to the national security of Estonia.

The cyberattacks linked to the Bronze Night lasted until May 19th. Thus, a total of 22 days (Figure 3; Pamment et al., 2019; Ottis, 2008). As the timing of the cyberattacks aligned with

the Bronze Night riots, and the chilled diplomatic relationships between Estonia and Russia, the Estonian Minister of Foreign Affairs blamed the Russian government for the attack. Nevertheless, according to NATO, there was no solid proof that these attacks were initiated or assisted by the Russian authorities (Herzog, 2011). In January 2008, one man was found guilty of the attacks. The Russian-Estonian student Dmitri Galuškevitš was fined (Ottis, 2008). However, it is unlikely that Galuškevitš executed the entire series of attacks by himself. During the first phase (April 27th to May 3rd), the attack had a more amateurish nature. There were instructions on how to engage in the Estonian cyberattacks on Russian forums (Ottis, 2008; Schmidt, 2013). Moreover, attacks originated from outside of Estonia, such as in Russia, Egypt, and the United States (Herzog, 2017). In the second phase (May 4th to May 19th), the attacks were executed more professionally. The attacks were performed by botnets, which are often more professionally used to conduct cyberattacks (Schmidt, 2013; Herzog, 2011).

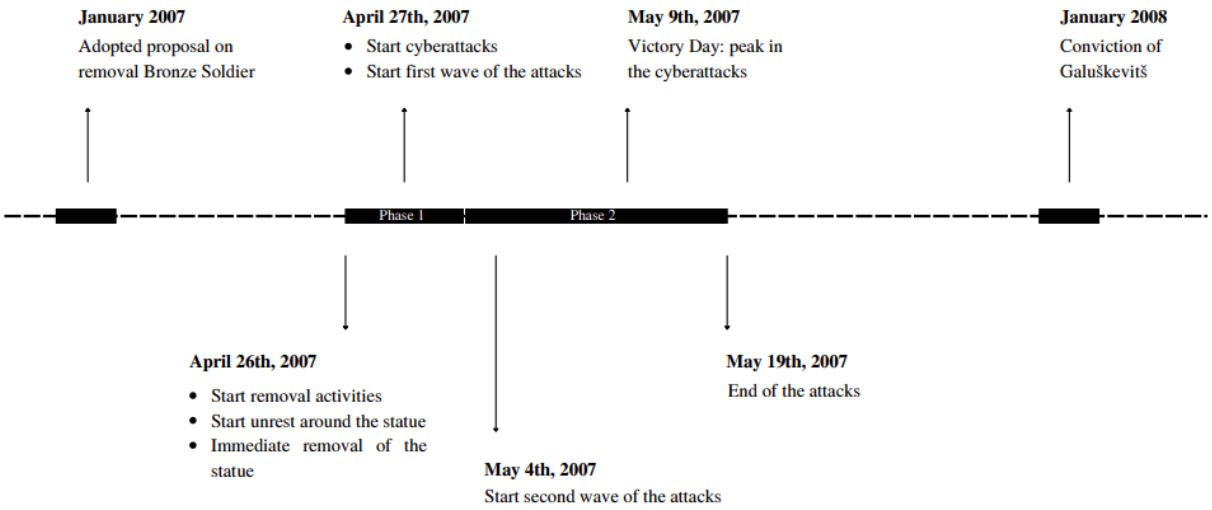


Figure 3. Timeline of the 2007 Cyberattacks on Estonia (Pamment et al., 2019)

Besides the level of professionalism, the targets also differed among the first and the second phase. In the first phase, mainly high-profile targets were attacked, such as the websites of the government, the president, and parliament. However, in the second phase, citizens were more directly targeted as two major banks became among the targets of the attack (Pamment et al., 2019). As Estonians were for 97% dependent on online banking, this second phase created more 'casualties' than the first phase (Pamment et al., 2019). The DDoS attacks disrupted the online activities of the major banks for 45 to 90 minutes. Furthermore, it was impossible to engage in international financial transactions. These attacks impacted Estonians more directly in their daily activities than disrupting activities on governmental websites (Pamment et al., 2019).

Altogether, this causes the 2007 Cyberattacks on Estonia to comply with the 3 characteristics of a rally event: I) an international focus; II) involve the country directly; and III) be short-term focused (Mueller, 2007). First, although the only person convicted was Estonian, the event took place in an international debate between Estonia and Russia, including the historical roots. Moreover, Estonia considered Russia their first suspect. Second, Estonia itself was attacked directly. The cyberattacks were focused on the Estonian government, parliament and president. Later, the attacks also moved to more intervention with the daily lives of the Estonian by attacking banks. Third, the attacks could be considered short-term. The total span of the attacks was 22 days and therefore, did not last longer than a month. Altogether, it could be argued that the cyberattacks were a rally event.

Although Estonia did not end up with significant damage resulting from the attacks, the cyberattacks were a wake-up call for many European countries and NATO (Tuohy, 2010). Both NATO and the EU discussed new cybersecurity doctrines, including sanctions as punishment for attacking nations (Herzog, 2011; Kovács, 2018). It eventually resulted in the Cyber Defence Management Authority and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (Herzog, 2011). The EU extended the activities of the European Union Agency for Cybersecurity and adopted a Digital Agenda for Europe, in which counteractivities are discussed (Herzog, 2011). Eventually, the EU adopted its cyber security strategy in 2013 (Kovács, 2018). For Estonia, the attacks changed the country into one of the leaders in cybersecurity (Tuohy, 2010; Joubert, 2012). For example, the NATO CCDCOE is based in Tallinn, and the international cyber study is called the 'Tallinn Manual' (Kovács, 2018)

Even though the cyberattacks on Estonia were the first series of cyber warfare attacks, they were not the last. In the last 15 years, several countries faced interstate cyberattacks, such as Georgia, Iran, Pakistan and India, and Saudi Arabia (Gazula, 2017; Dehlawi & Abokhodair, 2013; Shad, 2019; Kozlowski, 2014). More recently, since the Crimea annexation, Ukraine suffered several cyberattacks which intensified after the 2022 Russian invasion of Ukraine (Przetacznik & Tarpova, 2022). Additionally, Romania faced a series of DDoS attacks. These attacks are associated with the Russian invasion of Ukraine (Rosca & Fota, 2022; Cerulus, 2022). Whether these attacks were on purpose or spill-over effects, cyberattacks are among the main worries of Europe (Cerulus, 2022).

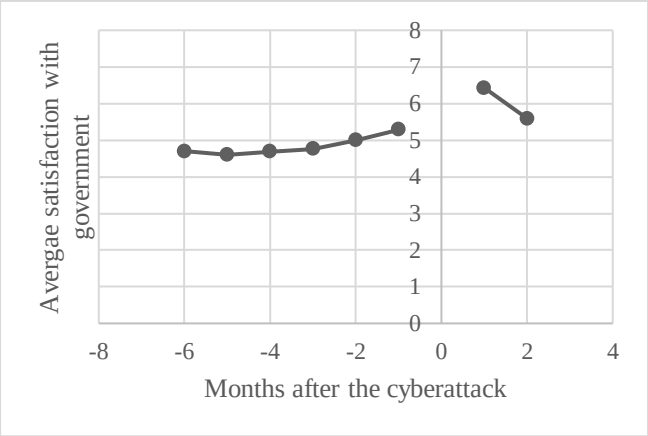
4. Analysis

As highlighted in the previous section, the Estonian cyberattacks covered two months (April and May) and two different phases, each with their own level of professionalism, targets and duration. In this analysis the attacks had, in total, a duration of 22 days (see figure 3). These attacks have in greater of lesser extent impacted the daily activities of the Estonian population. As mentioned, the attacks did not cause any significant damage, and therefore, its main aim was hitting the Estonian society or government via other means. This section examines whether these attacks had a societal impact via public support.

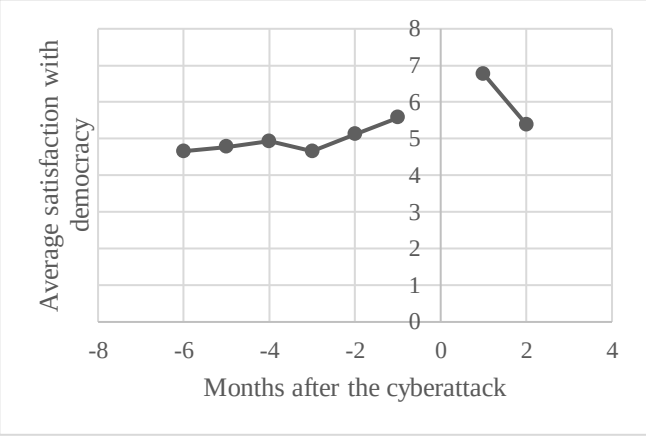
4.1 Results

The RD analyses show that the 2007 Cyberattacks had neither a significant impact on the population's satisfaction with the government nor democracy. The results of the analysis are summarized in table 3. Graph 1 illustrates the impact of the attacks on the average satisfaction with the current government. The graph shows a sharp increase in satisfaction with the government in the first month during the attacks. This point is also the highest average rating in the total dataset. However, in the second month, the average satisfaction dropped close to the baseline, similar to before the attack in April 2007. Nevertheless, the averages after the attack are higher (5.76) and the averages before the attack (4.73). Panel A, column 1 of table 3 shows the discontinuity of satisfaction with the current government before and after the cyberattack. The discontinuity is positive, but not significant: satisfaction with the current government is 0.665 points higher (SE 0.415) after the cyberattack than before. When the bandwidth of the analysis is reduced to data from March to May 2007, the results remain similar. Panel A, column 2 of table 3 shows that there is still a positive (0.583; SE 1.115) but no significant discontinuity.

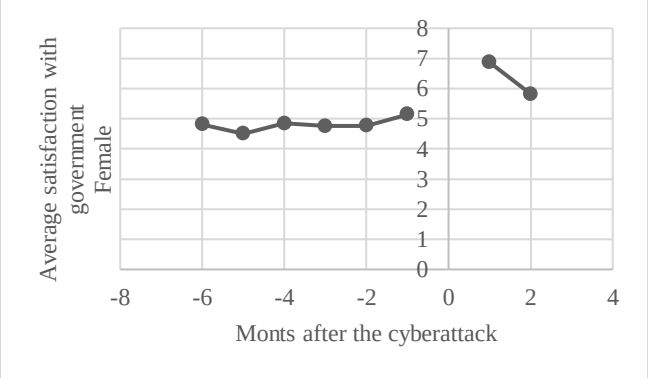
Graph 2 shows the difference in satisfaction with democracy before and after the cyberattack. Again, there is a sharp increase in the month after the attack. However, in the second month, these results drop below the latest rating before the attack. Like the previous results, the average rating of democracy after the attack is higher (5.68) than the rating before the attack (4.86). Table 3, column 1 of panel B shows a positive effect on the satisfaction with democracy after the cyberattack (0.214; SE 0.446). However, the effect is not significant. When the bandwidth is reduced, the effect remains positive but not significant (0.243; SE 1.132).



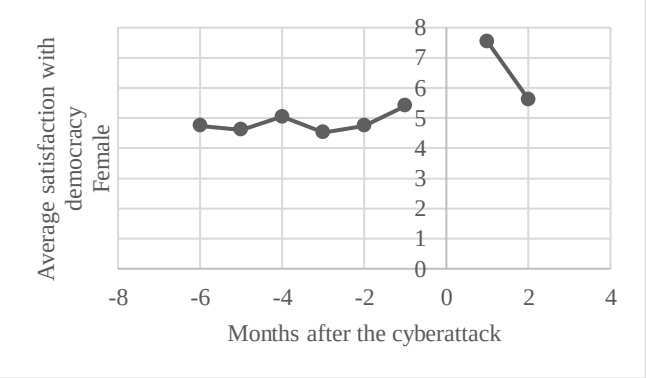
Graph 1. Average satisfaction with government before and after the cyberattack. Averages weighted by post-stratification weights



Graph 2. Average satisfaction with democracy before and after the cyberattack. Averages weighted by post-stratification weights



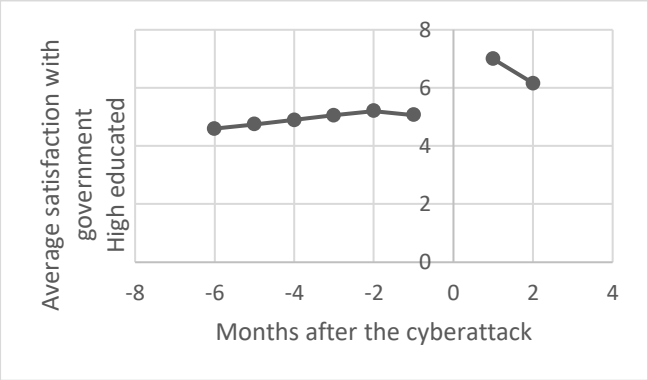
Graph 3. Average satisfaction with government, among women, before and after the cyberattack. Averages weighted by post-stratification weights



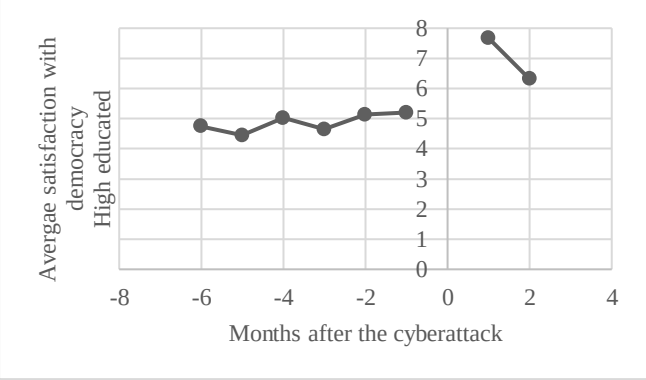
Graph 4. Average satisfaction with democracy, among women, before and after the cyberattack. Averages weighted by post-stratification weights

As shown in table 1, the balancing test shows a relatively equal distribution of individuals among the treatment and control groups. Based on these tested characteristics, four subgroup analyses are conducted. The first subgroup is women. Graphs 3 and 4 illustrate the average satisfaction ratings of government and democracy respectively among women. In both cases, there is again a sharp increase in the first month after the attack, which drops in the second month. Table 4, column 1 shows similar results. Overall, satisfaction with the current government is higher after the attack than before (1.213; SE 0.529). This effect is positive and significant ($p < 0.05$). The satisfaction with democracy is also higher after the attack than before (0.824; SE 0.577) but not significant among women.

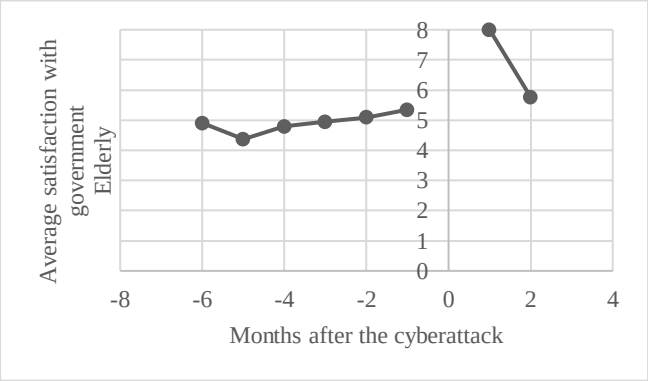
The second subgroup contains the higher-educated individuals. Graphs 5 and 6 (government and democracy respectively) show again an increase in the first months after the attack, which declines after. Table 4, column 2, presents again in both cases a positive increase, although not significant. Similar results are presented when analyzing only the elderly (table 4, column 3; graphs 7 & 8).



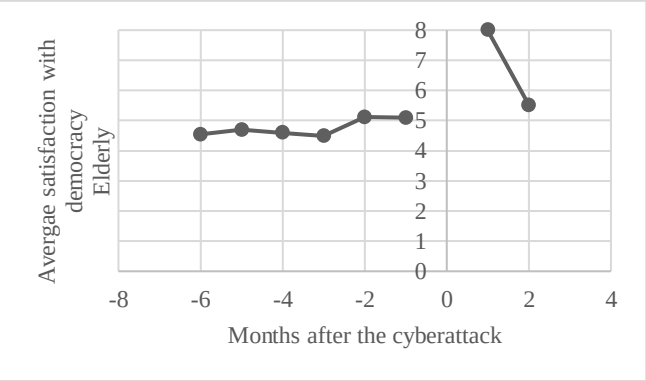
Graph 5. Average satisfaction with government, among high educated, before and after the cyberattack. Averages weighted by post-stratification weights



Graph 6. Average satisfaction with democracy, among high educated, before and after the cyberattack. Averages weighted by post-stratification weights

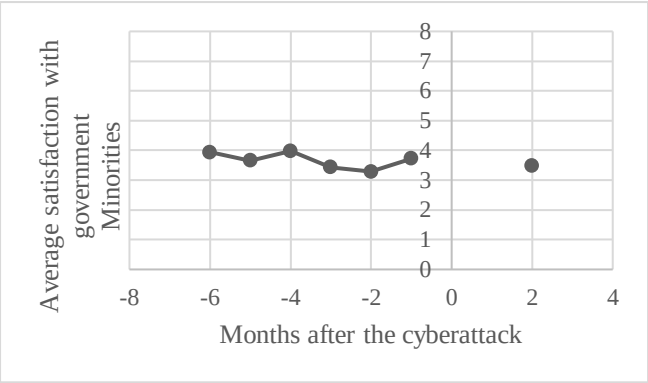


Graph 7. Average satisfaction with government, among elderly, before and after the cyberattack. Averages weighted by post-stratification weights

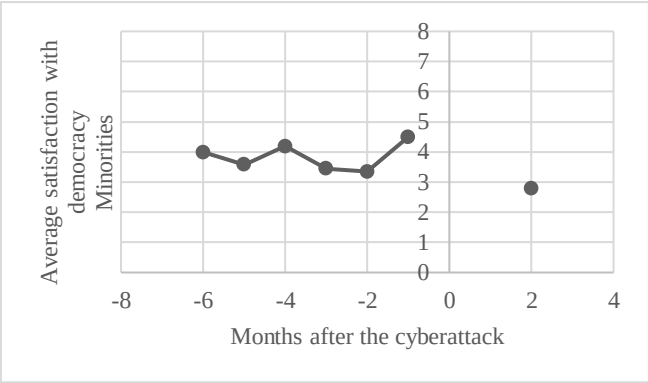


Graph 8. Average satisfaction with democracy, among elderly, before and after the cyberattack. Averages weighted by post-stratification weights

The last subgroup analyzed contains individuals belonging to an ethnic minority. These graphs show a different pattern (graphs 9 and 10). During the first month after the attack, there is a decrease in average satisfaction ratings compared to the previous measurement point. There is no indication of recovered levels in the second month, as this data is missing. Table 4, column 4, presents the analysis results. In the case of satisfaction with the government, there was a positive, non-significant effect of 0.476. Concerning satisfaction with democracy there was a negative, but the non-significant effect of 0.697.



Graph 9. Average satisfaction with government, among people beloning to minorities, before and after the cyberattack. Averages weighted by post-stratification weights



Graph 10. Average satisfaction with democracy, among people belonging to minorities, before and after the cyberattack. Averages weighted by post-stratification weights

Overall, the 2007 Cyberattacks had neither a significant effect on satisfaction with de government nor democracy. Nevertheless, in all cases (except the subgroup ethnic minorities), there was a visible increase in satisfaction in the first month of the attack. This peak in satisfaction ratings is always followed by a drop. As the observed effects are not significant, therefore both hypotheses are rejected. Considering the subgroup analyses, there is only a positive significant effect on satisfaction with the current government among women. In other words, the satisfaction with the government among women increased by 1.213 points after the 2007 Cyberattack compared to the overall satisfaction with the government before the attacks. Strikingly, the analysis of women on their satisfaction with democracy is not significant. All other subgroups have no significant effects as well.

	RDD All data (8 months) (1)	RDD 3 months (2)
Panel A. Before and after the attack		
Satisfaction with current government	0.665	0.583
	(0.415)	(1.115)
Months included	Oct 2006 – May 2007	March 2007 – May 2007
N	1402	207
Panel B. Before and after the attack		
Satisfaction with democracy	0.214	0.243
	(0.446)	(1.132)
Months included	Oct 2006 – May 2007	March 2007 – May 2007
N	1349	195

Table 3. Regression Discontinuity Analysis on Satisfaction with current government and Satisfaction with democracy
****Significant at the 1 percent level. **Significant at the 5 percent level. *Significant at the 10 percent level.*

	RDD Women (1)	RDD High educated (2)	RDD Elderly (3)	RDD Ethnic minority (4)
Panel A. Before and after the attack				
Satisfaction with current government	1.213**	0.647	0.940	0.476
	(0.529)	(0.697)	(0.676)	(1.293)
Months included	Oct 2006 – May 2007	Oct 2006 – May 2007	Oct 2006 – May 2007	Oct 2006 – May 2007
N	778	502	501	380
Panel B. Before and after the attack				
Satisfaction with democracy	0.824	1.081	0.762	-0.697
	(0.577)	(0.763)	(0.713)	1.397
Months included	Oct 2006 – May 2007	Oct 2006 – May 2007	Oct 2006 – May 2007	Oct 2006 – May 2007
N	749	494	464	379

Table 4. Regression Discontinuity Analysis on Satisfaction with current government and Satisfaction with democracy
****Significant at the 1 percent level. **Significant at the 5 percent level. *Significant at the 10 percent level.*

4.2 Discussion

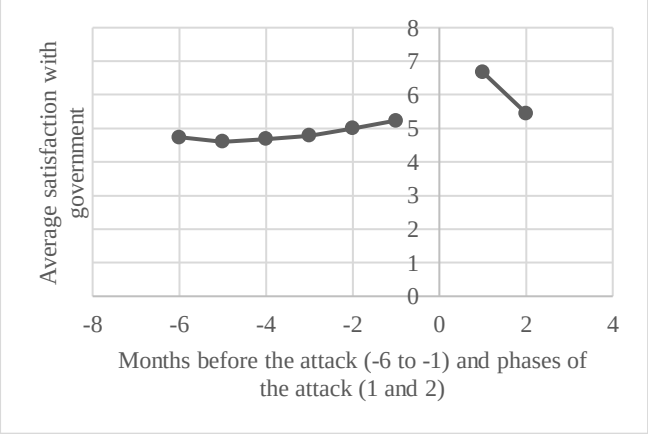
Generally, both analyses on satisfaction with the government, and satisfaction with democracy are positive but non-significantly improved after the cyberattacks. Therefore, both hypothesis I and II are rejected. Nonetheless, there is a visible peak in the first month of the attack, which declines in the second month of the attack. To explain this short peak and sudden decline in average satisfaction ratings, attention is dedicated to the events that happened during the cyberattacks.

4.2.1 The peak after the attack

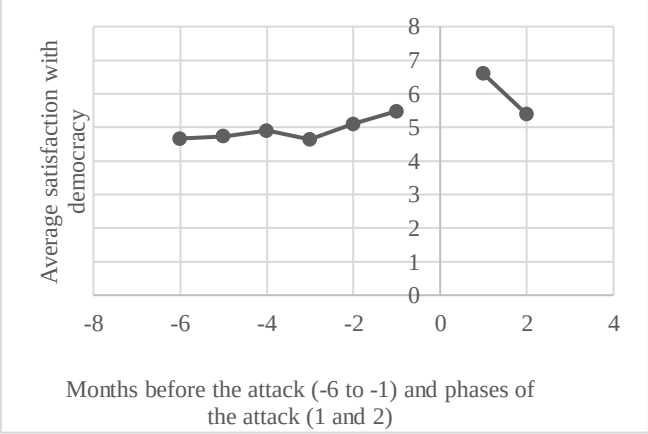
As mentioned, in the first month after the attack, there is a visible peak in both the satisfaction with the current government and with the democracy. In both cases is this peak also the highest satisfaction average of the entire sample. This sudden peak could be the effect of the rally event, as the cyberattacks comply to the three main characteristics: I) an international focus; II) involve the country directly; and III) be short-term focused. This might explain the sudden increase of the satisfaction ratings. The underlying mechanisms of this sudden increase are the quest of security, the overruling of other political affairs, and increased emotions of anger (Bækgaard, et al., 2020; Lambert, et al., 2011; Lambert, et al., 2010).

4.2.2 The downfall after the peak

After the peak of the attack, there is a visible decrease of the average satisfaction ratings for both the government as well as democracy. As mentioned, the cyberattacks can be distinguished in two phases: I) the more amateurish phase. During this period, the unweighted averages of satisfaction with the government and democracy are 6.67 and 6.60 respectively (N=15); and II) the more professional phase. The average satisfaction rates of both the



Graph 11. Average satisfaction with democracy (unweighted) in phase 1 and 2 of the attack



Graph 12. Average satisfaction with the government (unweighted) in phase 1 and 2 of the attack

government and democracy decrease visibly in this phase (5.45 and 5.39 respectively; N = 34). Graphs 11 and 12 illustrate the decline in satisfaction rates from the first to the second phase. The decline in average satisfaction ratings from phase one to phase two is clearly visible and contrasts with the earlier opted theory of rally events. This leads to the question why there is a sudden drop in satisfaction ratings while the cyberattack in still in place. First, an explanation could be the duration of the attack. Mueller (1970) argues that a rally event should be short term to increase the satisfaction ratings. However, when the event is not sharply focused and takes longer, it loses the attention of the population. Therefore, Mueller (1970) argues, that events that are no sudden change are not a rally event. Although a short-term, or sharply focused event is not defined explicitly, the 2007 attacks could fit both the box of short-term, as well as long term. This could explain why the ratings decline in the second phase. The first phase of the attack was a sudden shock. However, as the weeks passed and the cyberattack transpired, the satisfaction ratings declined. The underlying mechanisms of a rally event (security, overruling, anger) became less present.

Another explanation could be in the nature of the attacks. The first attack was performed in a more amateurish manner, while the second phase included the use of professional measures such as botnets (Ottis, 2008). The difference in the execution of the attacks among the phases could increase the feeling of insecurity. Similar effects are visible by physical terror attacks. The lone wolf attacks create less societal impact than attacks executed by terrorist organizations (Spaaij, 2010). Terrorist organizations often entail a more professional strategy, which includes planning and resources. Furthermore, the attacks executed by terrorist organizations often cause more victims than those of lone wolfs (Alakoc, 2015). When applying the 2007 Cyberattacks case to these terrorism theories, it might indicate that amateurish executed attacks are affecting society less than professional executed attacks. These amateurish attacks may have less impact on society in general, and therefore, affect the average satisfaction levels less.

Moreover, during the first phase the scope of the victims differed from the second phase. As mentioned, during the first phase, the victims were more high-profile (government websites and e-mail inboxes), while in the second phase, the population was more directly hit (attacking banks). Relating to targeting civilians, there was an increase of ‘casualties’ in this second phase. Again, when falling back on the terrorism theories, an increase in casualties also causes more societal effects (Alakoc, 2015). This could explain why the satisfaction ratings decrease when

entering the second phase. However, both in the case of the professionalism level and the scope of victims, the terrorism theories do not comply to the rally-theory.

4.2.3 Subgroup analysis

When analyzing the subgroup analyses, a similar pattern is visible as compared to the main analysis. Women, higher educated and elderly all show a sharp peak and a sudden drop. Thereby, they follow the general pattern. However, their average satisfaction ratings do differ from the general analysis.

When zooming in on the satisfaction ratings among women, there is a similar pattern to the general pattern. In the first month after the attack, the satisfaction rating peak, after which they quickly drop again. Overall, the average satisfaction ratings after the attack are still higher than before the attack, which is similar to the general satisfaction ratings. Thus, there is a positive effect of cyberattacks on the satisfaction ratings of both the government and democracy. Strikingly, the effect is larger among women, than among the overall sample. Before the attack, the average satisfaction levels are approximately the same as the general sample's satisfaction ratings. However, after the attack, women score their satisfaction with the government and democracy almost 0.5 higher on average than the general sample. The cyberattack seems to have a larger effect on women than on the general sample. Important to note is that the effect on satisfaction with the government among women is the only significant effect of all analyses. However, these results contradict the theory, which argues that women are overall less satisfied with democracy and incumbents, as they tend to have a more neutral attitude towards the two entities (Logan & Bratton, 2006; Hansen & Goenaga, 2019; Crow, 2010). The rally event had a bigger impact on women than expected. A possible explanation might be the enhanced feelings of fear, security or anger which are the main mechanisms behind a rally event (Bækgaard, et al., 2020; Lambert, et al., 2011; Lambert, et al., 2010). Yet, as there is no previous research on the effect of rally events on gender, it is not possible to explain these results. Therefore, this outcome is an interesting starting point for further research on the gendered differences when facing cyberattacks or rally events.

The trends among the elderly and higher educated are like those of the women. Both groups scored similarly before the attack compared to the general sample. However, after the attack, their satisfaction levels increase overall more than the general satisfaction levels. Based on the theory of satisfaction levels among the elderly, it is argued that the elderly have higher

satisfaction levels than the total population. Generally, older people are less neutral concerning their satisfaction with the democracy or incumbents. Therefore, they belong to the most satisfied and dissatisfied groups. However, more important is the role of historical awareness in this case study. Crow (2010) argues that historical memories of non-democratic times make the elder generation more satisfied with the current political situation. As the 2007 Cyberattacks on Estonia are a direct consequence of a conflict with strong historical roots (remembrance of the Soviet victory vs remembrance of Soviet domination), it is assumable that these memories play an important role in the increase of the satisfaction with government and democracy among the elderly.

Concerning the higher educated, the increased levels of satisfaction contradict the theory. As Wang (2005) and Almond and Verba (2015) argue, higher educated citizens have more political interests and awareness, which causes them to be more critical of their government functioning. Nevertheless, the higher educated were more satisfied than the general population. This assumes that the higher educated were less critical of their government. However, it could also assume that the higher educated had more understanding and knowledge of the political climate in which the cyberattacks took place. With this reasoning, it is more likely that the higher educated are more satisfied with their government and democracy than the general population, which might have less knowledge of the political situation.

Lastly, there is an interesting effect visible among the ethnic minority sample. Before the attack, this group shows lower satisfaction ratings than the general sample. After the attack, their satisfaction ratings dropped, which is a contrary effect compared to the main sample. According to the theory, two important mechanisms impact satisfaction ratings among minority groups. First, the psychological band with politics in their country. When this bond is stronger, their democratic satisfaction will also be higher, and vice versa (Inglehart & Carballo, 1997; Sanders et al., 2013). In earlier research, it was already shown that ethnic minorities in Estonia have lower satisfaction levels than the majority population (Chereson & Estes, 2022). Therefore, it is assumable that the ethnic minorities in Estonia have a relatively weak psychological bond with Estonian politics. Second, and possibly more important, is the mechanism of historical grievances. When there are many (historical) tensions between minority and majority groups, the satisfaction of the former will also be lower (Inglehart & Carballo, 1997). The background of the 2007 Cyberattacks on Estonia was the removal of the Bronze Soldier. For ethnic Russians, the statute reassembles the Soviet victory over Nazi

Germany and the fallen Soviet soldiers. The tension which the removal of the Bronze Soldier created was the origin of the riots, and the cyberattacks. As the Russians are the biggest minority group in Estonia, and they make up almost 25 percent of the total population, it is not surprising that their overall satisfaction levels drop during the start of the attacks. Nevertheless, in this case, it is doubtful if the drop in satisfaction is directly caused by the cyberattacks, or by the overall conflict over the Bronze Soldier.

Overall, it is uncertain what causes the difference in satisfaction ratings between April and May. To determine why the satisfaction rates dropped in May/phase 2, compared to April/phase 1, further research is necessary. Similar research could be performed on other cases of cyberwarfare attacks, to learn about the relationship between the attacks and the satisfaction with the government and democracy. Nevertheless, the RD analysis illustrated that, generally, there is no significant increase in satisfaction ratings of both the government and democracy before and after the attack. This rejects both hypotheses. Therefore, it is assumable, based on this case, that executing a cyberattack is not a sufficient means to decrease support for government or democracy.

The cause of a lack of effect of cyberattacks on public support for a government or democracy might lie with the case selection. As mentioned in the case study, during the first phase, the Estonian population was not directly hit by cyberattacks. Only indirectly, via government websites and news outlets, the Estonian society followed along with the attacks. During the second phase, banks were also targeted, which made the Estonian population victims as well. However, as only two major banks were hit, and the duration of these attacks were varying from 45 to 90 minutes each, it raises the question of to what extent the Estonian population was hit by the cyberattacks. Did these attacks disturb their daily activities as much as assumed in this paper? This might be an explanation for the non-result: if the Estonians were unknowingly victims of these attacks, they could not affect their public support for a government or democracy. Furthermore, the cyberattacks on Estonia consisted of multiple attacks, varying in length. There was no target attacked for 22 days straight. This might also decline the impact of cyberattacks in general. For example, it makes a difference in the impact of someone's life if a bank is unavailable for 22 days straight or 90 minutes. To measure whether the found non-result applies to all state-sponsored cyberattacks, it is necessary to redo this analysis on other cases of state-sponsored cyberattacks.

5. Conclusion

As daily and government activities are more online than ever, and (state-sponsored) cyberattacks are increasing, the question of to what extent this may affect political and societal affairs is more relevant than ever (Saleous et al., 2022). Although there has been a lot of research on cyberattacks, the effect of state-sponsored attacks on public support among the attacked population has faced little research (Chapman et al., 2011; Akoto, 2021; Agrafiotis et al., 2018; Musman et al., 2011). Nevertheless, there are examples of cyberattacks interfering with states with the motivation to change regimes or decrease incumbent support (Abrams, 2019; Reuters, 2022; Lis, 2020; Ellehuus, 2020; Brattberg & Maurer, 2018). By applying the rally-around-the-flag theory, this paper addressed the question of to what extent state-sponsored cyberattacks on states impact the public support.

To analyze the gap in the literature, this paper used the 2007 Cyberattacks on Estonia as a case. These attacks are considered the first time that a cyber warfare attack has been conducted (Pamment et al., 2019). Moreover, it was the start of the EU and NATO cybersecurity doctrines (Juurvee & Mattiisen, 2020; Kozlowski, 2014). By conducting a regression discontinuity analysis, the results revealed that there is no significant impact of cyberattacks on state-sponsored on either the populations' satisfaction with their government or the democracy in general. Therefore, both hypotheses are rejected: there is neither a positive nor negative significant impact of state-sponsored cyberattacks on public support.

These results lead to the question of cyberattacks having an impact on public support. According to the analysis, the attacks do not impact public support. Nevertheless, there is a visible increase in both satisfaction levels with the current government as well as democracy in the first month after the attack. However, these satisfaction levels drop near the pre-attack levels in the second month. This might indicate that there is a sudden, but non-significant, effect close to the start of the attack.

But why does this effect disappear in the second month? A possible result of this lies within the rally-around-the-flag theory itself. It might be that the attack takes too long to retain the mechanisms under the rally theory. The urge for security, overruling of other affairs, and increased anger diminish, and public support for the government and democracy declined as

well. Other possible explanations lay within the case itself, such as the level of professionalism of the attacks, and the scope of the victims.

To determine the effect of a cyberattack further research is needed. The current sample only measured respondents before and during the attack. There is more data needed to determine whether the satisfaction levels remain on the pre-attack level, increase, or decrease after the end of the attack. In other words, this analysis only provides a small part of the overall satisfaction levels, but it cannot determine to what extent the cyberattacks might play a role in the long term, for example when deciding whether to vote for the incumbent government during new elections.

Nevertheless, although this analysis is only focused on 2007 Cyberattacks in Estonia and worked with limited data, it is striking that the attacks neither had a positive nor negative significant effect on the public support of the Estonians. According to the rally-around-the-flag theory, these attacks should increase Estonian satisfaction levels significantly. Contrarily, when executed right, the attacks are aimed to diminish Estonian satisfaction levels. To understand this non-result and determine whether the attacks do affect public support in other cases or the long term, further research is needed.

Bibliography

Abrams, A. (2019, 18 april). Here's What We Know So Far About Russia's 2016 Meddling. *Time*. https://time.com/5565991/russia-influence-2016-election/

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Angrist, J. D. & Pischke, J. (2014). *Mastering 'Metrics: The Path from Cause to Effect* (with French flaps). Princeton University Press.

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Alakoc, B. P. (2015). Competing to Kill: Terrorist Organizations Versus Lone Wolf Terrorists. *Terrorism and Political Violence*, *29*(3), 509–532. https://doi.org/10.1080/09546553.2015.1050489

Almond, G. A. & Verba, S. (2015). *The Civic Culture - Political Attitudes and Democracy in Five Nations: Political Attitudes and Democracy in Five Nations* (New ed). Amsterdam University Press.

Asamoah, J. K. (2018). The concept of agency theory in electoral democracy. *Journal of African Elections*, 66–82. https://doi.org/10.20940/jae/2018/v17i2a4

Baekgaard, M., Christensen, J., Madsen, J. K., & Mikkelsen, K. S. (2020). Rallying around the flag in times of COVID-19: Societal lockdown and trust in democratic institutions. *Journal of Behavioral Public Administration*, *3*(2). https://doi.org/10.30636/jbpa.32.172

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Blais, A., Bol, D., Giani, M., & Loewen, P. J. (2020). COVID-19 lockdowns have increased support for incumbent parties and trust in government. *LSE*. https://blogs.lse.ac.uk/politicsandpolicy/

Blank, L. R. (2013). International Law and Cyber Threats from Non-State Actors. *Israel Yearbook on Human Rights, Volume 43 (2013)*, 111–139. https://doi.org/10.1163/9789004242081_006

Bowles, S., Carlin, W., & Stevens, M. (2017). Unit 5 Property and power: Mutual gains and conflict. In *The Economy*.

Brantly, A. F. (2014). Cyber Actions by State Actors: Motivation and Utility. *International Journal of Intelligence and CounterIntelligence, 27*(3), 465–484. https://doi.org/10.1080/08850607.2014.900291

Brattberg, E. & Maurer, T. (2018). RUSSIAN ELECTION INTERFERENCE: Europe′s Counter to Fake News and Cyber Attacks. In *Carnegie Endowment for International Peace*. Carnegie Endowment for International Peace. Geraadpleegd op 13 december 2022, van https://www.jstor.org/stable/resrep21009.6

Center for Strategic and International Studies. (2022, december). *Significant Cyber Incidents*. Geraadpleegd op 13 december 2022, van https://csis-website-prod.s3.amazonaws.com/s3fs-public/221212_Significant_Cyber_Events.pdf?5RVe0CglJK0dJqGjblIJeHORD95oJ_QW

Cerulus, L. (2022, February 23). Cyber ‘spillover’ from Ukraine looms in the Baltics. *POLITICO*. https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/

Chanley, V. A., Rudolph, T. J., & Rahn, W. M. (2000). The Origins and Consequences of Public Trust in Government. *Public Opinion Quarterly*, *64*(3), 239–256. https://doi.org/10.1086/317987

Chapman, I. M., Leblanc, S. & Partington, A. (2011). Taxonomy of cyber attacks and simulation of their effects. *Annual Simulation Symposium*, 73–80. https://doi.org/10.5555/2048558.2048569

Chereson, P. & Estes, K. W. (2022). Paradoxes of minority representation: a comparison of Russophone political attitudes in Estonia and Latvia. *Journal of Baltic Studies*, 1–19. https://doi.org/10.1080/01629778.2022.2150667

Chowanietz, C. (2010). Rallying around the flag or railing against the government? Political parties’ reactions to terrorist acts. *Party Politics*, *17*(5), 673–698. https://doi.org/10.1177/1354068809346073

Crow, D. (2010). The Party’s Over: Citizen Conceptions of Democracy and Political Dissatisfaction in Mexico. *Comparative Politics*, *43*(1), 41–61. https://doi.org/10.5129/001041510x12911363510358

De Juan, A. & Pierskalla, J. H. (2014). Civil war violence and political trust: Microlevel evidence from Nepal. *Conflict Management and Peace Science*, *33*(1), 67–88. https://doi.org/10.1177/0738894214544612

Dehlawi, Z., & Abokhodair, N. (2013). Saudi Arabia’s response to cyber conflict: A case study of the Shamoon malware incident. *2013 IEEE International Conference on Intelligence and Security Informatics*. https://doi.org/10.1109/isi.2013.6578789

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy. *Networks and Netwars. The Future of Terror, Crime and Militancy*, 239–288.

Dinicu, A. (2014). Cyber threats to national security. Specific features and actors involved. *Buletin Scientific*, *2*(38).

Ellehuus, R. (2020, juli). Did Russia Influence Brexit? *Center for Strategic and International Studies*. Geraadpleegd op 13 december 2022, van https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit

European Social Survey. (2018). ESS8 Codebook edition 1.0. europeansocialsurvey.org. https://www.europeansocialsurvey.org/docs/round8/survey/ESS8_appendix_a7_e01_0.pdf

European Social Survey. (n.d.-a). About ESS | European Social Survey (ESS). europeansocialsurvey.org. https://www.europeansocialsurvey.org/about/

European Social Survey. (n.d.-b). ESS4-2008. europeansocialsurvey.org. Retrieved December 2, 2022, from https://ess- search.nsd.no/en/study/c7f5d299-6bb6-4d4b-b9b5-f52b3026a9a4

Fearon, J. D. (1999). Electoral Accountability and the Control of Politicians: Selecting Good Types versus Sanctioning Poor Performance. In A. Przeworski, *Democracy, Accountability, and Representation* (pp. 55–97). Cambridge University Press.

Ferejohn, J. (1986). Incumbent performance and electoral control. *Public Choice*, *50*(1–3), 5–25. https://doi.org/10.1007/bf00124924

Gabel, M. & Hix, S. (2005). Understanding Public Support for British Membership of the Single Currency. *Political Studies*, *53*(1), 65–81. https://doi.org/10.1111/j.1467-9248.2005.00517.x

Gailmard, S. (2014). Accountability and Principal–Agent Theory. In M. Bovens, R. Goodin, & T. Schillemans, *The Oxford Handbook of Public Accoutability* (pp. 90–105). Oxford University Press.

Gazula, M. (2017). *Cyber Warfare Conflict Analysis and Case Studies* [Master Thesis]. Massachusetts Institute of Technology.

General Intelligence and Security Service. (2021). Annual Report AIVD 2021. In *Ministry of Interior and Kingdom Relations*. AIVD.

Hansen, M. A. & Goenaga, A. (2019). Gender and Democratic Attitudes: Do Women and Men Prioritize Different Democratic Institutions? *Politics & Gender, 17*(1), 23–52. https://doi.org/10.1017/s1743923x19000473

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Herzog, S. (2017). Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity. *Georgetown Journal of International Affairs*, *18*(3), 67–78. https://doi.org/10.1353/gia.2017.0038

Huang, H. H. (2018). Exploring Citizens' Hierarchical Government Satisfaction: Evidence from China and Taiwan. *Japanese Journal of Political Science*, *19*(2), 122–145. https://doi.org/10.1017/s1468109918000026

Hughes, D., & Colarik, A. (2017). The Hierarchy of Cyber War Definitions. *Intelligence and Security Informatics*, 15–33. https://doi.org/10.1007/978-3-319-57463-9_2

Hunter, L., Albert, C. D. & Garrett, E. (2021). Factors That Motivate State-Sponsored Cyberattacks. *The Cyber Defense Review*, *6*(2), 111–128. https://www.jstor.org/stable/10.2307/27021379

Inglehart, R. & Carballo, M. (1997). Does Latin America Exist? (And Is There a Confucian Culture?): A Global Analysis of Cross-Cultural Differences. *PS: Political Science and Politics*, *30*(1), 34. https://doi.org/10.2307/420668

Joubert, V. (2012). *Five years after Estonia's cyber attacks: lessons learned for NATO?* NATO Defense College. Retrieved December 2, 2022, from https://www.files.ethz.ch/isn/143191/rp_76.pdf

Juurvee, I., & Mattiisen, M. (2020). The Bronze Soldier Crisis of 2007. In *icds.ee*. International Centre for Defence and Security. Retrieved December 2, 2022, from https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf

Kadivar, M. (2014). Cyber-Attack Attributes. *Technology Innovation Management Review*, *4*(11), 22–27. https://doi.org/10.22215/timreview/846

Kavallieros, D., Germanos, G., & Kolokotronis, N. (2021). Profiles of Cyber-Attackers and Attacks. In *Cyber-Security Threats, Actors, and Dynamic Mitigation* (1st ed.). CRC Press.

Katz, G. & Levin, I. (2015). The Dynamics of Political Support in Emerging Democracies: Evidence from a Natural Disaster in Peru. *International Journal of Public Opinion Research*, *28*(2), 173–195. https://doi.org/10.1093/ijpor/edv010

Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, *116*, 102493. https://doi.org/10.1016/j.simpat.2022.102493

Kotzian, P. (2010). Public support for liberal democracy. *International Political Science Review*, *32*(1), 23–41. https://doi.org/10.1177/0192512110375938

Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review*, *23*(1), 16–24. https://doi.org/10.2478/raft-2018-0002

Kozlowski, A. (2014). COMPARATIVE ANALYSIS OF CYBERATTACKS ON ESTONIA, GEORGIA AND KYRGYZSTAN. *European Scientific Journal, ESJ*, *10*(7).

Lagos, M. (2003). Support for and Satisfaction with Democracy. *International Journal of Public Opinion Research*, *15*(4), 471–487. https://doi.org/10.1093/ijpor/15.4.471

Lambert, A. J., Scherer, L. D., Schott, J. P., Olson, K. R., Andrews, R. K., O'Brien, T. C., & Zisser, A. R. (2010). Rally effects, threat, and attitude change: An integrative approach to understanding the role of emotion. *Journal of Personality and Social Psychology*, *98*(6), 886–903. https://doi.org/10.1037/a0019086

Lambert, A. J., Schott, J. P., & Scherer, L. (2011). Threat, Politics, and Attitudes. *Current Directions in Psychological Science*, *20*(6), 343–348. https://doi.org/10.1177/0963721411422060

Lewis, J. A. (2010). The Cyber War Has Not Begun. *Center for Strategic and International Studies*, *3*, 1–4.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lis, J. (2020, 21 juli). Was there Russian meddling in the Brexit referendum? The Tories just didn't care. *The Guardian*. https://www.theguardian.com/commentisfree/2020/jul/21/russian-meddling-brexit-referendum-tories-russia-report-government

Logan, C. & Bratton, M. (2006). THE POLITICAL GENDER GAP IN AFRICA: SIMILAR ATTITUDES, DIFFERENT BEHAVIORS. *AFROBAROMETER WORKING PAPERS*, 1–29. https://www.afrobarometer.org/wp-content/uploads/2022/02/AfropaperNo58.pdf

Lu, M., & Reeves, J. (2014). *Types of Cyber Attacks* [Slide show]. TCIPG.org. http://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf

Manin, B., Przeworski, A., & Stokes, S. C. (1999). Elections and Representation. In *Democracy, Accountability, and Representation* (pp. 29–54).

McAllister, I. & White, S. (2014). Electoral Integrity and Support for Democracy in Belarus, Russia, and Ukraine. *Journal of Elections, Public Opinion and Parties*, *25*(1), 78–96. https://doi.org/10.1080/17457289.2014.911744

Minority Rights Group. (2021, 5 februari). *Russians*. https://minorityrights.org/minorities/russians-3/

Mueller, J. E. (1970). Presidential Popularity from Truman to Johnson. *American Political Science Review*, *64*(1), 18–34. https://doi.org/10.2307/1955610

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, *140*(4), 70–92. https://doi.org/10.1162/daed_a_00116

Musman, S., Tanner, M., Temin, A., Elsaesser, E. & Loren, L. (2011). Computing the impact of cyber attacks on complex missions. *2011 IEEE International Systems Conference*. https://doi.org/10.1109/syscon.2011.5929055

Nazario, J. (2009b). Politically Motivated Denial of Service Attacks. *The Virtual Battlefield: Perspectives on Cyber Warfare*, 163–181. https://doi.org/10.3233/978-1-60750-060-5-163

Nielsen, J. H., & Lindvall, J. (2021). Trust in government in Sweden and Denmark during the COVID-19 epidemic. *West European Politics*, *44*(5–6), 1180–1204. https://doi.org/10.1080/01402382.2021.1909964

Olsen, J. P. (2016). Democratic accountability and the terms of political order. *European Political Science Review*, *9*(4), 519–537. https://doi.org/10.1017/s1755773916000084

Osawa, J. (2017). The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*, *24*(2), 113–131. https://doi.org/10.1080/13439006.2017.1406703

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In R. Ottis (Ed.), *Proceedings of the 7th European Conference on Information Warfare*. Academic Publishing Limited.

Pamment, J., Sazonov, V., Granelli, F., Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Gravelines, J., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Sari, A., Simons, G. & Terra, J. (2019). Hybrid Threats: 2007 cyber attacks on Estonia. In *Stratcomcoe.org*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86

Przetacznik, J., & Tarpova, S. (2022). Briefing: Russia's war on Ukraine: Timeline of cyber-attacks. In *www.europarl.europa.eu* (PE 733.549). European Parliamentary Research Service. Retrieved December 2, 2022, from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

Reuters. (2022, 7 november). Russia's Prigozhin admits interfering in U.S. elections. *Reuters*. https://www.reuters.com/world/us/russias-prigozhin-admits-interfering-us-elections-2022-11-07/

Rosca, M., & Fota, A. (2022, March 18). Romania hit with cyberattacks at start of Ukraine war, official says. *POLITICO*. https://www.politico.eu/article/europe-cyber-security-russia-ukraine-romania/

Rosenzweig, P. (2011). Cybersecurity and Public Goods: The Public/Private "Partnership." *Emerging Threats Essays*, 1–36.

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R. & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2022.06.005

Sanders, D., Fisher, S. D., Heath, A. & Sobolewska, M. (2013). The democratic engagement of Britain's ethnic minorities. *Ethnic and Racial Studies*, *37*(1), 120–139. https://doi.org/10.1080/01419870.2013.827795

Schandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, 1–16.

Schmidt, A. (2013). The Estonian Cyberattacks. *A Fierce Domain: Conflict in Cyberspace*, 174–193. http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf

Schmidtt, M. N. (2016). Conduct of hostilities. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. New York: Cambridge University Pres.

Sekhon, J. S. & Titiunik, R. (2017). On Interpreting the Regression Discontinuity Design as a Local Experiment. *Advances in Econometrics*, 1–28. https://doi.org/10.1108/s0731-905320170000038001

Shad, M. R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. *Strategic Studies*, *39*(1), 1–19. https://doi.org/10.53532/ss.039.01.00115

Spaaij, R. (2010). The Enigma of Lone Wolf Terrorism: An Assessment. *Studies in Conflict & Terrorism*, *33*(9), 854–870. https://doi.org/10.1080/1057610x.2010.501426

Stecker, C. & Tausendpfund, M. (2016). Multidimensional government-citizen congruence and satisfaction with democracy. *European Journal of Political Research*, *55*(3), 492–511. https://doi.org/10.1111/1475-6765.12147

Stevens, M., Bowles, S., & Sethi, R. (2017). Markets, efficiency, and public policy. In *The Economy*.

Stoker, G., Evans, M. & Halupka, M. (2018). Trust and democracy in Australia. In *Democracy 2025* (Report No.1). Democracy 2025. Geraadpleegd op 12 december 2022, van https://apo.org.au/sites/default/files/resource-files/2018-12/apo-nid208536.pdf

Tapon, F. (2018, July 7). The Bronze Soldier Explains Why Estonia Prepares For A Russian Cyberattack. *Forbes*. https://www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=3232343e98c7

Toshkov, D. (2016). *Research Design in Political Science*. Macmillan Publishers.

Tuohy, E. (2010). Toward an EU Cybersecurity Strategy: The Role of Estonia. In *International Centre for Defence Studies*. Retrieved December 2, 2022, from https://icds.ee/wp-content/uploads/2013/Toward%20an%20EU%20Cybersecurity%20Strategy%20-%20The%20Role%20of%20Estonia.pdf

Valentino, B., Huth, P. & Balch-Lindsay, D. (2004). "Draining the Sea": Mass Killing and Guerrilla Warfare. *International Organization*, *58*(02). https://doi.org/10.1017/s0020818304582061

Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boekee, S., Koppen, L., Van den Berg, B., De Bos, A., & Van der Lubbe, J. (2015a). On (the emergence of) cyber security science and its challenges for cyber security education. *The NATO STO/IST-122 Symposium*, 1–10.

Van den Berg, J. (2015b). Wat maakt cyber security anders dan informatiebeveiliging. *Magazine Nationale Veiligheid En Crisisbeheersing, (2) 2015*, *2*, 4–5.

Wang, Z. (2005). Before the Emergence of Critical Citizens: Economic Development and Political Trust in China. *International Review of Sociology*, *15*(1), 155–171. https://doi.org/10.1080/03906700500038876

Weimann, G. (2004). Cyberterrorism: How real is the threat? *United States Institute of Peace*, *119*.

Zmerli, S. & Newton, K. (2008). Social Trust and Attitudes Toward Democracy. *Public Opinion Quarterly*, *72*(4), 706–724. https://doi.org/10.1093/poq/nfn054

Appendix I Dataset Description

The dataset is the entire round 3 of the European Social Survey, conducted between October 2006 and May 2007. The dataset does not include external added variables. Nevertheless, the dataset has been cleaned up.

1. By hand, the variable ‘treatment’ is added. Treatment indicates whether the respondent answered the survey before of during the cyberattacks. Thereby 0 indicates before the cyberattack and 1 indicates during the cyberattack.
2. Moreover, other variables have been recoded to make the evaluation easier. This includes the following variables: “Belong to minority ethnic group in country”, “Gender”, “Highest level of education”, “Age of respondent, calculated”, “How satisfied with the national government”, and “How satisfied with the way democracy works in country”.
3. One case has been deleted from the dataset. This respondent had answered the survey in December 2007. As this is outside of the duration of the survey, this date might have been a coding mistake. Nevertheless, it is impossible to discover the actual date of this survey. Therefore, this case has been deleted.

Appendix II Descriptive Statistics

```
/*************
> 2. Descriptives
> 2b. Means, Treatment = 1 (treatment group)
> *************/
. mean(pdwrk) [pweight=pspwght] if Treatment ==1

Mean estimation                 Number of obs   =        49
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
       pdwrk |    .561948   .0728044       .415565     .708331
------------------------------------------------------------


. mean(eduyrs) [pweight=pspwght] if Treatment ==1

Mean estimation                 Number of obs   =        49
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
      eduyrs |   12.57098   .4080936      11.75045    13.39151
------------------------------------------------------------


. mean(edulvla) [pweight=pspwght] if Treatment ==1

Mean estimation                 Number of obs   =        49
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
     edulvla |   3.221384   .1732823      2.872976    3.569791
------------------------------------------------------------


. mean(agea) [pweight=pspwght] if Treatment ==1

Mean estimation                 Number of obs   =        49
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
        agea |   44.77716   2.850758      39.04532    50.50899
------------------------------------------------------------
```

```
. mean(gndr) [pweight=pspwght] if Treatment ==1

Mean estimation                 Number of obs   =        49
--------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+------------------------------------------------
        gndr |   .5929753   .0728098      .4465814    .7393692
--------------------------------------------------------------

. mean(ctzcntr) [pweight=pspwght] if Treatment ==1

Mean estimation                 Number of obs   =        49
--------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+------------------------------------------------
     ctzcntr |   .9084186   .0441042      .8197413     .997096
--------------------------------------------------------------

. /************

> 2. Descriptives
> 2c. Means, Treatment = 0 (control group)
> ************/
. mean(pdwrk) [pweight=pspwght] if Treatment ==0

Mean estimation                 Number of obs   =      1,467
--------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+------------------------------------------------
       pdwrk |   .5919039   .0130242      .5663558     .617452
--------------------------------------------------------------


. mean(eduyrs) [pweight=pspwght] if Treatment ==0

Mean estimation                 Number of obs   =      1,465
--------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+------------------------------------------------
      eduyrs |   12.26561   .0731851      12.12205    12.40917
--------------------------------------------------------------
```

```
. mean(edulvla) [pweight=pspwght] if Treatment ==0

Mean estimation                 Number of obs   =      1,467
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
    edulvla |   3.335543   .0290631      3.278534    3.392553
------------------------------------------------------------

. mean(agea) [pweight=pspwght] if Treatment ==0

Mean estimation                 Number of obs   =      1,465
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
       agea |   45.52469   .5073699      44.52944    46.51994
------------------------------------------------------------

. mean(gndr) [pweight=pspwght] if Treatment ==0

Mean estimation                 Number of obs   =      1,467
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
       gndr |   .5483411   .0132632      .5223242    .5743579
------------------------------------------------------------

. mean(ctzcntr) [pweight=pspwght] if Treatment ==0

Mean estimation                 Number of obs   =      1,466
------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+----------------------------------------------
    ctzcntr |    .77845   .0110638      .7567475    .8001526
------------------------------------------------------------
```

```
/************
> 2. Descriptives
> 2d. Means: stfdem stfgov
> ************/
. mean(stfdem) [pweight=pspwght]

Mean estimation                 Number of obs   =      1,349
--------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+------------------------------------------------
      stfdem |   4.891605   .0623678      4.769256    5.013953
--------------------------------------------------------------


. mean(stfgov) [pweight=pspwght]

Mean estimation                 Number of obs   =      1,402
--------------------------------------------------------------
             |       Mean   Std. Err.     [95% Conf. Interval]
-------------+------------------------------------------------
      stfgov |   4.764165    .058382       4.64964    4.878691
--------------------------------------------------------------

. /************
> 2. Descriptives
> 2e. tabulate: stfdem stfgov
> ************/
. tabulate (stfdem)

How satisfied with the |
way democracy works in |
               country
 |      Freq.     Percent        Cum.
-----------------------+-----------------------------------
extremely       |         57        4.23        4.23
dissatisfied
                  1 |         44        3.26        7.49
                  2 |        102        7.56       15.05
                  3 |        195       14.46       29.50
                  4 |        150       11.12       40.62
                  5 |        283       20.98       61.60
                  6 |        162       12.01       73.61
                  7 |        175       12.97       86.58
                  8 |        123        9.12       95.70
                  9 |         41        3.04       98.74
Extremely       |         17        1.26      100.00
satisfied
-----------------------+-----------------------------------
              Total |      1,349      100.00
```

. tabulate (stfgov)

How satisfied with the national government

Freq.	Percent	Cum.
Extremely dissatisfied	45	3.21	3.21
1	41	2.92	6.13
2	117	8.35	14.48
3	219	15.62	30.10
4	180	12.84	42.94
5	305	21.75	64.69
6	182	12.98	77.67
7	153	10.91	88.59
8	108	7.70	96.29
9	33	2.35	98.64
Extremely satisfied	19	1.36	100.00
Total	1,402	100.00	