October 2018 · Dr. Sven Herpig, Julia Schuetze, supported by Jonathan Jones

Securing Democracy in Cyberspace

An Approach to Protecting Data-Driven Elections

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Inhalt

Introduction 3

Strategic Motivations 6
- Manipulate the Outcome 7
- Delegitimize the Democratic Process 7
- Discredit Political Stakeholders 8
- Intimidate a Government 9
- Erode International Credibility 10

Election Hacking Tactics 10
- Denial 12
- Erosion 12
- Reconnaissance 14
- Leaks 14
- Persuasion 15
- Blackmail 16

Data-Driven Electoral Process 17
- Publicly Accessible Electoral Data 18
- Personal Data 19
- Self-Reported Data 21
- Government-Issued Data 23
- Personal Communication Data 24
- Security Data 24

Conclusion 27

Election Security Recommendations and Good Practices 28
- I. Effective implementation of election security 28
- II. Organization of election security 29
- III. Security mechanisms to secure election infrastructure 29
- IV. Capacity building for key stakeholders and the public 31
- V. Strategic communications to create resilience 32
- VI. International Cooperation on Election Security 33

Acknowledgement 34

Annex A: Attack Vectors 35

1. Introduction

Elections are the cornerstone of democracy. Vulnerabilities in the electoral process increased vastly due to the all-encompassing digitization that took place in the last decade. For every democratic country, it is imperative to maintain a free and fair electoral process, thus protecting it from "interference". Interference in this analysis is limited to activities that leverage hacking operations regardless of the adversary (domestic and foreign). Other studies have used interference in the context of disinformation. This paper however focuses on assessing adversarial motivations and hacking methods as well as the vulnerabilities of the data-driven electoral process. Protecting the electoral process means more than just increasing information security of voting machines, however. This paper asserts that at its core, it is all about security of data in the entire electoral process, which is data that can be exploited by adversaries. Safeguarding the electoral process entails protecting relevant data and designing mitigation techniques in case these security measures fail. Therefore, democracies must not only improve information security, but also increase society's resilience to election interference. Due to the nature of the problem, solutions require the involvement of various actors: a whole-of-nation approach.

In modern representative democracies, politicians and political parties are supposed to represent the people. By governing on their behalf, they derive their legitimacy from the people through periodic, free and fair elections[1]. Elections are therefore one of the fundamental pillars of democracy. Accordingly, protecting elections is imperative to democracy. The electoral process entails more than just casting a vote in a democratic society. To have free and fair elections, the activities of candidates, their parties and political campaigns leading up to election day, as well as the publication of the results afterwards, must have both actual and perceived integrity from interference. Because the electoral process is an integral part of democracy, any impediment to exercising the right to vote or tampering with the electoral process in any way is perceived as a serious threat to state sovereignty. This has not stopped governments in the past from interfering with foreign elections, however[2]. To deter these incursions and guard against them when they

1 United Nations, Resolution 52/129 Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization and Inter-Parliamentary Council, Declaration on Criteria for Free and Fair Elections.

2 Scott Shane, Russia Isn't the Only One Meddling in Elections. We Do It, Too.

occur, the integrity of elections has been historically protected by national and international law[3].

Today's debate about protecting the integrity of elections is not new. What is new is the threat that derives via cyberspace: the resulting scale in terms of remote threat projection, faster and more widespread dissemination of election relevant information and novel means of deception. Political parties, campaigns, and election infrastructure have digitized and therefore come to increasingly dependent on data, using big data algorithms to comb through voter rolls for targeted campaign advertisements to utilizing social media platforms to spread campaign messages, implementing online voter registration or casting the vote digitally; technology has proliferated in the political space. While this data-driven approach brings efficiency and accessibility to the electoral process, it also creates a number of risks. Increasingly, digitizing the electoral process and moving it online broadens the attack surface, which might be further exacerbated by emerging technologies, thereby increasing the vulnerabilities of and interferences to the electoral process.

Threat actors seek to take advantage of unique characteristics of the cyber domain which give them a high level of anonymity and flexibility to operate. The importance of addressing these threats is underlined by the fact that it is anticipated that threat actors will continue to refine and adapt their techniques[4]. Additionally, if interference in the electoral process through hacking proves impactful, more state and non-state actors might strive to acquire the skills and tools to conduct such intrusions. The truism that cyber offense is always one step ahead of cyber defense seems to be even more true when it comes to the electoral process. There are several reasons for this: firstly, even a failed attempt at or claims of election meddling through hacking can undermine the legitimacy of the electoral process if it becomes public because of the perception of vulnerability. This puts the defender, usually the state, at a distinct disadvantage. Another disadvantage is that

3 "Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State" -United Nations, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Declaration on Friendly Relations) and Jacqueline Van De Velde, The Law of Cyber Interference in Elections.

4 U.S. Director of National Intelligence report Assessing Russian Activities and Intentions in Recent US Elections.

the safeguards to protect election technologies against hacking interference are not sufficient yet.

Governments and key actors in the electoral process around the world have not been sufficiently prepared for election meddling leveraging hacking operations[5] and invested too little to protect their electoral process from cyber threats[6]. The hack of the Democratic National Committee (DNC) and the email hack and leak targeting John Podesta, Chairman of the 2016 Hillary Clinton presidential campaign, during the run-up of the 2016 US presidential elections[7] and the following disinformation campaign[8] need to serve as a wake up call to strategically think about the problem. Quite a few initiatives are doing this now. Most are either focusing on battling disinformation campaigns, campaign security, regulating political advertising or on increasing the information security of election IT systems[9]. There is no doubt that those approaches are crucial to protecting the electoral process. This paper however tackles the challenge from a slightly different angle, focusing on the various ways that hacked data related to an election could be exploited to interfere with the electoral process. The scope is slightly broader in the sense that the analytical framework puts emphasis on the security of the relevant data, thus develop recommendations to increase national security and society's resilience against interference. In addition to security, resilience is a feature of this paper's recommendations, since it is likely that a dedicated adversary will sooner or later be able to exploit election-related data. Recommendations should therefore not be limited to information security measures but also include propositions on strategic communication[10]. Go-

5 Jacqueline Van De Velde, The Law of Cyber Interference in Elections.

6 The divisive 2016 U.S. Presidential election saw almost $2.1 Billion raised in campaign funds with only a fraction of this actually spent on securing the IT systems the campaigns depended on -Center for Responsive Politics, 2016 Presidential Race campaign funding by candidate and Center for Responsive Politics, Expenditures Breakdown for the Clinton campaign.

7 Sven Herpig, Cyber Operations: Defending Political IT-Infrastructures.

8 U.S. Department of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System.

9 Belfer Center for Science and International Affairs, Harvard Kennedy School Defending Digital Democracy Releases New Playbooks for States to Counter Election Cyberattacks and Information Operations.

10 Belfer Center for Science and International Affairs, Election Cyber Incident Communications Plan Template: International Edition.

vernments need to be prepared for this to be able to maintain the legitimacy of the electoral process.

In the first section, the paper presents a threat analysis pertaining to why an adversary (whether domestic or foreign) – would seek to interfere with the electoral process. The assessment continues with portraying election hacking tactics that have been derived from election and political interference operations, and how they meddle with the information security in the electoral process. It distinguishes between immediate effects that can only be countered by improving information security and indirect effects which can additionally be hindered by resilience measures. The following section then assesses the kinds of data that exist throughout the electoral process and how accessible they are for a threat actor: whether they are publicly available (e.g. website hosting a party's political agenda) or not (e.g. an internal campaigning strategy). The data's accessibility shifts the threat model and thereby has an impact on security and resilience recommendations.

Therefore, this paper proposes that different security and accessibility levels of data have to be considered when designing corresponding security and resilience measures. It recommends a whole-of-nation approach involving media, political stakeholders, government and companies handling citizens/voter data.

2. Strategic Motivations

The first step towards protecting the electoral process in cyberspace is to understand the adversary's motivation for interfering. Though the (geopolitical) goals are certainly interrelated and hard to differentiate, we identified five major motivations why an adversary might target the data-driven electoral process: manipulation of outcome, delegitimization of the democratic process, discrediting political stakeholders, intimidation of a government and erosion of international credibility. Thus, this section offers a rather broad perspective of the geopolitical motivations for interfering with the electoral process through cyber means. Looking at those possibilities leads to the assumption that the attacker has one major advantage. Even a failed attempt to, for example, manipulate the votes might, if it becomes public, still erode public trust in the democratic process.

Manipulate the Outcome

Manipulation of the election outcome is the most most impactful way to meddle with an election; it is therefore also the most obvious one when it comes to leveraging hacking operations. Manipulating the outcome refers to interfering with the processes by which an individual, after having decided whom to support, casts a vote. Practices by which this could be done include altering the votes on any level (local, state, federal), as well as manipulating the voter databases or e-poll books and thereby disallowing a subset of eligible voters to cast their ballot for a particular politician or party. It works in both ways, either by making sure that a certain politician or party wins or, when there are more than two options, that a particular party or politician does not win the election. An adversary would conduct an attack against systems holding the aforementioned data to change the votes or voter data in the registration database such as address or party affiliation. In some countries, if the address is changed, voters might not be able to vote in their district or receive the ballot for vote by mail. If the party affiliation is altered, they might not be able to vote in party-related polls such as primaries (United States) or coalition treaties (Germany). The attacker might even go one step further and try to leverage operators that have access to any of those systems and force them to assist them in this endeavour.

Delegitimize the Democratic Process

Delegitimizing the democratic process means to introduce doubt that the electoral process is functioning as it is meant to through hacking operations – successful or not. The perception that the IT systems and infrastructures used in the election process are vulnerable to attacks or have been tampered with[11] delegitimizes the democratic process. This does not require a manipulation of the actual voting machines as long as the electorate believes that the outcome of the election does not reflect free and fair elections without interference. This effect can be achieved by attacking websites holding election-, campaign- or party-related data to deny the electorate from accessing that information or simply to call into question the integrity of the information. A similar operation could be carried out against systems holding relevant

11 "It has been publicly reported that Russian actors targeted electoral infrastructure in over 20 states prior to the 2016 election. Although there is no evidence indicating that these cyber operations resulted in the disruption of any voting results, the Russian government maintains both the intent and capability to undermine confidence in the integrity of an electoral tally. The need to increase cybersecurity among the nation's electoral infrastructure, and particularly in voter registration databases and electronic voting machines, has gained heightened salience since the 2016 election.", Suzanne Spaulding, Countering Adversary Threats to Democratic Institutions.

voter authentication information, which would delay the electorate's ability to vote. The voter databases could also be attacked and altered, so that voters would not be able to cast their votes[12] or would have to go through an additional verification process. To decrease trust in the system (rather than favor/disfavor a candidate or party), the attack does not need to target a certain subset of voters. As long as the manipulation becomes publicly known, it potentially harms the legitimacy of the process. Another way to decrease trust in the election system would be to expose, but not necessarily exploit, security flaws for example in voter databases, tallying software[13] or voting machines. It is however of utmost importance to find and patch those vulnerabilities, but they have to be disclosed in an orderly manner, following established coordinated vulnerability disclosure guidelines.

All of those attacks can be combined with the (targeted) spreading of news about the insecurity of the technology that enables the election process. What makes this effect so powerful is not only the broad range of tools with which it can be achieved, but also that once trust in the process is lost, it is difficult to regain. Therefore, successfully delegitimizing the democratic process can potentially yield a sustained impact and does not necessarily require a hacking operation to be successful – the appearance of a successful operation could already cause damage[14].

Discredit Political Stakeholders

Discrediting political stakeholders such as politicians, parties, interest groups or the current government can be a powerful tool to nudge public opinion to achieve a certain election outcome. Hacking operations can be used as a tool to achieve this goal in the data-driven electoral process. The most obvious of practices to achieve this is to use cyber means to obtain and release information or documents which make political stakeholders look bad, even going as far as causing a scandal. While just leaking documents seems like the "lazy" approach, spinning stories around them and/ or targeting a specific subset of people (e.g. through micro-targeting) can be scaled. Additional impact can be caused by altering documents and mixing them with originals. Furthermore, websites or social media accounts can be taken over

12 Nicole Perlroth, Michael Wines and Matthew Rosenberg, Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny.

13 Laura Smith-Spark, Hackers warn of flaws in German election software weeks before vote.

14 Even though it is out of scope for this analysis, the mere claim of a successful hacking operation against the election IT-systems and infrastructures might yield similar results (but would constitute an information operation/ disinformation campaign).

by an attacker and used to spread harmful information. This approach yields disadvantages for the defender, since debunking false stories takes time and is rarely as successful as spreading them[15]. In addition to discrediting single political stakeholders, attackers can also aim to discredit a set of political stakeholders such as a multi-party government or the established system of political stakeholders, also referred to as "the establishment." This can be achieved by discrediting a political idea all of them share, for example. The rise of the right-wing parties in Europe at the expense of the established and more moderate parties is based to a certain degree on discrediting their policy approach, among others. to deal with the refugee crisis[16]. Any of the stakeholders mentioned or their affiliates can also be targeted and then blackmailed, for example by sharing or publishing confidential data about others which in turn can be used to discredit those.

Intimidate a Government

A hack against the electoral system can be used to intimidate the targeted government as a geopolitical show of force, but does not necessary have to occur during the electoral process. It may, for example, be conducted during the runup to elections or international negotiations. Such a show of force would rather be about covertly relaying displeasure with a targeted government's national agenda, or sending a message such as "not even your elections are safe from us". The case of Ukraine's 2014 elections presents a rather overt attempt at intimidation through hacking. A well-coordinated, three-prong attack was conducted. It began with threat actors deleting key files on Ukraine's Central Election Commission computers four days before the presidential elections[17]. While the deletion of files was fixed the next day, minutes before the election results were announced on live television, malicious software was discovered that was meant to falsely portray the vote in favor of the ultra right-wing candidate. The third part of the attack was a distributed denial-of-service attack on the vote tallying system which delayed the final tally of the vote. It is difficult to independently assess the success of such an intimidation.

15 Soroush Vosoughi Deb Roy and Sinan Aral, The spread of true and false news online
Alexander Sängerlaub, Feuerwehr ohne Wasser?
Alexander Sängerlaub, Miriam Meier and Wolf-Dieter Rühl, Fakten statt Fakes

16 Simon Shuster, European Politics Are Swinging to the Right.

17 Mark Clayton, Ukraine election narrowly avoided 'wanton destruction' from hackers.

Erode International Credibility

Eroding the international credibility of the state's election process potentially leads to challenges in international relations and negotiations for that state, although we note that there have not been any empirical studies of this so far. If the integrity of a state's election can be challenged, the credibility of its government diminishes. Dealing with governments with questionable legitimacy can potentially cause a domestic and international backlash. For the affected state that can mean everything from having a slightly more difficult stance in bilateral and multilateral negotiations to states preferring to deal with the opposition and non-government stakeholders in the country and in the worst case exclusion from membership in certain international organizations[18]. On the international level, two aspects are vital and can be heavily impacted through election interference. First, the state needs to be able to follow through with commitments it makes on the international level. It must have the domestic support to implement policies, which means for example that there are no talks about reelections. Second, other states must be able to deal with a government without running the risk that the public opinion within their own electorate will turn hostile, due to dealings with an "illegitimate" government. Additionally, international development missions by the targeted state to assist other countries in developing democratic institutions could be undermined.

3. Election Hacking Tactics

This section introduces election hacking tactics which have either been observed in past election interference activities or broader political interference operations. Election hacking tactics are implemented, individually or in combination, to achieve the strategic goals discussed in the last section. To limit the scope of this paper, all tactics are based on hacking operations[19] leveraging traditional attack vectors[20]. For example, a persuasion/ disinformation campaign is only part of these election hacking tactics if it is connected to a hacking operation. This could be the case when the campaign includes micro-targeting that relies on stolen voter data or when it distributes/ leaks confidential data which has previously been obtained through a hack. Limi-

18 European Commission, Conditions of Membership.

19 Hacking is defined here as the exploitation of existing vulnerabilities in soft- and hardware and online services to access data in transit and data at rest or manipulate a target's device (e. g. by switching on sensors or altering existing software) -Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers.

20 See Annex A.

ting the scope to scenarios including hacking operations allows us to apply the CIA triad[21], a conventional analytical frame for security analysis. The CIA concept helps to assess whether the core aspects of information security, the Schutzziele[22] – confidentiality, integrity, availability or any combination thereof – have been breached. This paper applies the CIA principles to focus on the security of data that is part of the electoral process. The following analysis of the election hacking tactics highlights which CIA aspect is being targeted by which scenario.

There are two distinct categories of effects that can be identified in the election hacking tactics. The first category of effects are direct, which can be used to describe attacks that are conspicuous in nature and have immediate effects. An example for this would be targeting a candidate's website with a distributed denial-of-service, so that people cannot open the site and access information about the candidate on their platform anymore. Immediate effects can be countered through information security safeguards (e.g. firewalls, intrusion detection software, encryption, etc).

The second category of attacks are the ones in which the hacking operation itself does not cause a direct disruption to a target but can rather have a second tier effect. For example, in the run up to the 2017 French Presidential election, threat actors published information, some of which they apparently manipulated, gained from compromising IT systems of presidential candidate Emmanuel Macron's party "En Marche!"[23]. There was no immediately visible effect of the hack but leaking the obtained data was a second tier effect. While increased information security might have protected the party's IT systems, there was little it could have done about the leaking after the hack had already been carried out. This increases the difficulty for defenders to create proper defense mechanisms. It requires mitigating aspects such as strategic communication to increase the resilience of the electoral process. In this example, the party did however respond to the delayed effect by means of strategic communication, claiming that some of the leaked data and been forged or altered.

21 Chad Perrin, The CIA Triad.

22 Schutzziel (German): A goal to be achieved for protecting something. In information security, the Schutzziele are confidentiality, integrity and availability of information.

23 Andy Greenberg, Hackers hit Macron with huge email leak ahead of French Election.

Denial

Denial operations are ultimately about decreasing the availability of data. Websites, social media platforms, email accounts, messengers and physical IT infrastructures facilitate the flow of information to an electorate. A threat actor can interrupt this flow, thus denying (a subset) of voters access to or receipt of information. Such an attack can be used against political parties and candidates as well as against public political IT infrastructures, such as those providing information about the the electoral process in general. For example, this type of effect was achieved either knowingly or unknowingly by suspected hacktivists when they conducted a coordinated distributed denial-of-service attack on two key publicly-funded websites in the run up to the Dutch national election in 2017[24]. These two websites were used by nearly 50% of the eligible voter base in 2012 to help decide for which candidate to vote[25]. A recent example is Knox County, Tennessee, where hackers afflicted computer systems with a denial-of-service attack, led to a delay in disclosing results of the May 1st primary for local races, including sheriff and mayor[26].

Even though it is quite a different matter, denial operations could also be carried out against voting machines. In that case it would not deny people access to information, but rather impede their ability to vote. Rendering voting machines inoperable would deny (parts of) the electorate the right to vote. This would target firstly the integrity of data needed for the voting machines to be functional, and secondly the availability of voting machines and thus ultimately the votes. Denial operations have a direct effect.

Erosion

This tactic is mainly targeting the integrity of data crucial to the electoral process and the public perception of election security. Eroding trust in the electoral process can either be a direct objective or an unexpected byproduct of a successful hacking operation. The latter is the case when the revelation of an attack leads to doubt among the public as to whether the electoral system's integrity has been compromised or not. In either case, it is a direct effect of the hacking operation. The target within the electoral system can be anything from showing how vulnerable voting machines are[27] to an exposure

24 Harrison Van Riper, Turk Hack Team and the "Netherlands Operation".

25 Reuters Staff, Dutch voting guide sites offline in apparent cyber attack.

26 Travis Dorman, Cyberattack crashes Knox County election website; votes unaffected.

27 Adam Lusher, Hackers breached defences of US voting machines in less than 90 minutes.

of the voter registration database[28], which would also violate the confidentiality of data. The illusion of a compromised electoral system alone can cause severe damage to public trust and is worsened by (domestic) stakeholders wanting to take advantage of it. The gravity of this threat was emphasized in the cyberspace portion of the 2017 U.S. National Security Strategy paper[29]. This mode of attack has special potential to be used by cyber terrorists who look to incite fear among a populace[30].

Manipulation

Manipulation is all about targeting the integrity of data. Altering information, such as voter registration rolls, can be a subtle way for threat actors to achieve effects without drawing too much attention to their actions. This makes for an ideal setting for an attack on political campaigns that are increasingly depending on this information to define their campaign strategies[31]. This type of attack was seen during the 2014 Ukraine elections[32]. If those manipulations remain undiscovered for some time, it might be very difficult – even with backups – to reinstate the original versions of the altered files and documents. It would require precise knowledge about when exactly data was altered.

This tactic causes damage by eroding trust in the electoral process, even if it is discovered and mitigated. It can also be conducted almost entirely overtly – as it does not target availability or confidentiality – and matched with a persuasion campaign. Physical access to voting machines[33] (e. g. in transit) or supply chain attacks against the used hardware[34] are two out of several methods that can be used against voting machines to change votes or render the machines inoperable. Germany in 2009[35] as well as the Netherlands and Norway in 2017[36] choose to forgo electronic vote counting machines and ins-

28 James Temperton, The Philippines election hack is 'freaking huge'.

29 White House, National Security Strategy of the United States of America, December 2017.

30 James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War, and other Cyber Threats.

31 Sasha Issenberg, How Obama's Team Used Big Data to Rally Voters.

32 Mark Clayton, Ukraine election narrowly avoided 'wanton destruction' from hackers.

33 Lily Hay Newman, To Fix Voting Machines, Hackers Tear Them Apart.

34 John Sebes, Elections + National Security = Hardware Threats + Policy Questions.

35 Bundesverfassungsgericht, Verwendung von Wahlcomputern bei der Bundestagswahl 2005 verfassungswidrig.

36 Thomas Nilsen, Norwegian votes to be counted manually in fear of election hacking and Sewell Chan, Fearful of Hacking, Dutch Will Count Ballots by Hand.

tead hand count ballots in order to mitigate this type of threat to the public's trust in their the electoral processes. During the runup to the 2017 German elections, hackers also found ways to manipulate the software used for the collation and transmission of the voting results[37]. It shows that even if the actual vote is paper ballot based, there are ways to interfere with the results by conducting hacking operations.

Reconnaissance

Reconnaissance is mainly targeting the confidentiality of data, trying to compromise and to gain a foothold within a system for monitoring and future exfiltration. Therefore, as a byproduct, it violates integrity for example by establishing persistent backdoor access. When considering a target to hack, threat actors may seek to do a preliminary survey of a target's IT systems and its response mechanisms. Reconnaissance can serve as a staging point for threat actors to map out what additional vulnerabilities a target's IT system has and/or to monitor ongoing communications and data within the system. An important objective would be to covertly maintain access to the systems without being discovered, and establish a basis for additional effects such as manipulation. A possible second tier effect would be that trust in the system will be eroded if later on, for example through a security audit, it will be discovered that crucial IT systems or infrastructures were compromised, even though no election-related data was manipulated. This tactic was seen inter alia during the 2016 U.S. presidential elections, where threat actors were involved in targeting activity which involved probing election-related systems for vulnerabilities in 21 states[38].

Leaks

Leaks are mainly targeting the confidentiality of data. Leaking is focused on gaining compromising information on a target and then publishing or leaking the information to a third party to further obfuscate the threat actor's intentions and possibly increase the credibility of the stolen material. In the past for example, Wikileaks has served as an ideal platform to pass information to the public that was obtained through hacking[39]. Even though it would be ideal to find a credible platform that publishes the leaked documents, any platform – bundled with emails to journalists and social media distribution – will do. This type of attack received widespread attention during the 2016

37 46halbe, Software zur Auswertung der Bundestagswahl unsicher und angreifbar.

38 Morgan Chalfant, Bipartisan group of lawmakers backs new election security bill.

39 Joseph Cox, Guccifer 2.0 Claims Responsibility for WikiLeaks DNC Email Dump.

U.S. Presidential election, as the timed leak of compromising information cast doubt on impartiality of the DNC candidate nomination process and caused the chairwoman of the Democratic National Committee to resign[40]. This leak operation possibly also factored into the very close outcome of the general election[41]. Even if victims of this type of attack have remained above reproach in their actions, the leak case involving French President Emmanuel Macron's party "En Marche!" shows that threat actors will go so far as to manipulate the integrity of the data in order to disparage a target[42]. From a strategic communication perspective, the party appears to have been prepared for such a case[43]. The hacking operation targeting the German Bundestag in 2015 showed that a hacking operation does not necessarily have to be followed by a leak of the obtained data – even though it was believed that it will be exploited during the following elections[44]. The activity that creates impact during this operation is not the hack itself but the leak, therefore making it a second tier effect.

Persuasion

Persuasion relies on targeting the confidentiality of data, be it private conversations and documents, personal information or account data. The difference to leaks is that persuasion is targeted and custom-tailored. This tactic can work in different ways. First, valid documents obtained through a hacking operation can be used as core for a broader disinformation campaign – as what happened with the Podesta emails[45]. Disinformation campaigns are often spun around a real document or event. Secondly, persuasion could work through a micro-targeted campaign propagating false narratives relying on voter data gained from a prior hack – e. g. from a compromised election system vendor, as happened in the U.S.[46]. Lastly, hostile takeovers of accounts, such as social media accounts, could help threat actors in gaining a level of credibility among a targeted group of voters and to push out certain messages or discredit the owner of such an account as happened to

40 Edward-Isaac Dovere and Gabriel Debenedetti, Heads roll at the DNC.

41 Sven Herpig, Cyber Operations: Defending Political IT-Infrastructures.

42 Adam Nossiter, David E. Sanger and Nicole Perlroth, Hackers Came, but the French Were Prepared.

43 Andy Greenberg, Hacker Hit Macron with Huge Email Leak Ahead of French Election.

44 Sven Herpig, Cyber Operations: Defending Political IT-Infrastructures.

45 Raphael Satter, Inside story: How Russians hacked the Democrats' emails.

46 Matthew Cole, et al, Top Secret NSA Report Details Russian Hacking Efforts days before 2016 Election.

Australia's Defence Industry Minister Pyne in 2017[47]. The attack surface for persuasion is very broad, it causes second tier effects and can be linked to several other election hacking tactics. Considering that hacking operations at some point will be successful and the points that can be leveraged by an adversary are numerous, the best course of action to counter persuasion threats might be to increase the society's resilience to them.

Blackmail

This tactic leverages the confidentiality of data and can for example be used to achieve the intimidation of a government. While threat actors may tend to focus attacks on the systems that underpin democratic processes, it should not be ruled out that political actors themselves serve as attractive targets to threat actors. An attack on key political actors could yield compromising information to threat actors that could be used to blackmail or disparage candidates and parties. While those "hack-mail" activities for financial gain have been observed in the past in non-political contexts, it is reasonable to assume that they will be conducted for political gains in the future – especially with the latest developments concerning ransomware[48]. The hack of Ashley Madison and subsequent leak of its intimate and incriminating data led to a number of blackmail cases. Criminals leveraging this data threatened to expose the infidelity and asked for money in return[49]. Instead of asking for money, they could have also asked for political favors. A targeted hack of a politician's or their family's digital devices[50] could yield confidential data that, when exposed, harms the reputation of the politician, his campaign, party or the government as a whole. The same scenario could be leveraged against administrators of election related IT systems such as voting machines. Concerns about political hack-mail increased last year after the alleged Russian hacking operations against U.S. targets[51] and the UK parliament[52]. Blackmail clearly causes second tier effects that can be substantially delayed.

47 Fergus Hunter, 'I was hacked!': Christopher Pyne's Twitter account in porn mishap.

48 Lily Hay Newman, The Ransomware That Hobbled Atlanta Will Strike Again.

49 Alex Hern, Spouses of Ashley Madison users targeted with blackmail letters.

50 Natasha Bertrand, Hacked Text Messages allegedly sent by Paul Manafort's daughter discuss 'bloody money' and killings, and a Ukrainian Lawyer wants him to explain.

51 Kenneth P Vogel, David Stern and Josh Meyer, Manafort faced blackmail attempt, hacks suggest.

52 Ben Riley-Smith, Blackmail fears after Parliament hit by 'sustained and determined' cyber attack on MPs' email network.

Election Hacking Tactics	**Effect**	**Primarily Affected *Schutzziel*[1]** **C**onfidentiality, **I**ntegrity and/or **A**vailability of Data
Denial	Direct	Availability *Secondary: Integrity*
Erosion	Direct	Integrity *Secondary: Confidentiality*
Manipulation	Direct and Second Tier	Integrity
Reconnaissance	Second Tier	Confidentiality *Secondary: Integrity*
Leaks	Second Tier	Confidentiality *Secondary: Integrity*
Persuasion	Second Tier	Confidentiality
Blackmail	Second Tier	Confidentiality

Table 1. Election hacking tactics within the CIA Triad

4. Data-Driven Electoral Process

While the strategic motivations present the general driving force of adversaries to meddle with the electoral process, the assessment of the election hacking tactics demonstrates how the vulnerabilities of the data-driven electoral process can be exploited. The election hacking tactics used examples of data that has been targeted and how it was or could be exploited in an interference campaign. While this description of data was still generic, the following section presents the entirety of data relevant to the electoral process to more clearly map out the attack surface.

Data plays a key role in democratic elections and informs the process. Political parties increasingly rely on digital tools that digest data for their campaigns, technology to help facilitate the voting process of casting votes, counting votes and checking off voters[53] and election offices use office management tools to prepare the elections[54]. It is considered that most data

53 Nicole Perlroth et al, Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny.

54 Shannon Vavra, There's more than one way to hack an election.

types are not solely made for election purposes but are distributed more broadly in other contexts of society. That is to say, not all data is the same. Therefore, this section analyses what kind of data is available in the election process and what it is used for. Additionally, it identifies whether the data is publicly available or not, linking it to the CIA triad. This is a major consideration when thinking about how it can be exploited and therefore what countermeasures could be applied.

Publicly Accessible Electoral Data

Publicly accessible electoral data is information that is created as part of the election process and/or specifically for it. Depending on the country, this form of electoral data may include statistics on the political party affiliation of electors, election results, tabulations of votes for ballot measures or candidates from previous elections by voting area as well as information about campaign funding[55]. Electoral data is for example present in the process of drawing electoral boundaries that is digitised in some countries (USA[56], Mexico, India[57]) and requires inter alia census and global population data, maps and sometimes the voting history of electors. Another example for publicly accessible electoral data are all information and media displayed on websites within a election context, such as campaign websites or the official website of a local election office. This kind of data has already become a target for hackers. In a recent hack on the day of the primary election in Knox County in Tennessee hackers used a distributed Denial of Service attack to make the website, thus information on the website (publication of vote count), inaccessible. Later it was found that this was done to distract from another form of attack that targeted the web server software[58] which holds other types of data. In another example, the election website of Lee County, Florida was hacked and an anti-ISIS message with vulgar language was placed on the homepage[59]. In Venezuela, a hacker named Sepúlveda allegedly

55 Allegedly Russian attackers stole information from a Tennessee campaign donation website during their 2016 interference operation. Reported by Eric Geller, 60 Minutes DHS election security report - part 1 and part 2.

56 Ace Project, 1990 Census of Population And Housing P.L. 94-171 Redistricting Data.

57 Ace Project, Electoral districts for greater accountability.

58 Zaid Shoorbajee, Election day website crash in Knox County coincided with more direct hack, report says.

59 Dave Elias, Update left Lee County Elections Website vulnerable to hackers.

sent screenshots to the campaign showing how he had hacked then presidential candidate Chávez's website and could turn it on and off at will[60].

Publicly accessible electoral data can be found in a variety of places (academic institutions, government agencies[61], polling companies, media outlets, website hosters, non-government organisations[62]...). It is not designed with confidentiality in mind as it has the purpose to create transparency of the election process, but it should be available and valid. When information about a certain politician's/party's platform or the election as such cannot be accessed anymore, the free and fair election process might be affected. Additionally, tampering with the integrity of publicly accessible electoral data can result in changing people's perceptions or spreading false narratives.

Personal Data

Personal data is information about an individual, relating to an identified or identifiable natural person[63]. Campaigns and governments collect a significant amount of personal data about voters and this data could be exploited by threat actors. Such exploits could result for example in identity theft or in the use of that data to target individuals with disinformation about the election, about candidates or political parties, or about important issues at stake in the election[64].

Personal data is relevant throughout the whole electoral process and is tied to specific activities. For example, voter registration that includes information such as the address, date of birth, gender or eye color can be relevant for identifying a person, while email addresses are pieces of personal information that may not readily identify a voter but could serve the purpose of reaching a voter. Political parties rely on this kind of personal data for their targeted campaigning efforts. This can include a voter's income level or reli-

60 Tim Maurer and Agustin Rossi, Why Latin America Needs to Prepare Now for Election Meddling.

61 Federal Election Commission, Contributions to All Candidates.

62 Center for Responsive Politics, Follow The Money, A Handbook.

63 Definitions vary, but this paper uses the General Data Protection Regulation since it is a broad definition, EUGDPR.org, GDPR FAQs What constitutes personal data.

64 Moreover, this data could be exploited for identity theft, identifying de-identified data and physical harm to the individual (these are residential home addresses, not PO Boxes, meaning people that face threats of physical harm (victims of domestic violence, stalking victims, judges, law enforcement officers, etc.) may find that they need to move if their address is breached).

gious affiliation. Even the type of car a person drives is seen by political parties as a factor correlated to voting preference for a specific party. While at first glance it may seem that this data has little to do with the electoral process, it has now become a crucial factor in determining who parties aim to reach with their message[65]. Moreover, the use of personal biometric details for voter identification has steadily increased[66]. Currently[67], 35% of over 130 surveyed Electoral Commissions worldwide capture biometric data as part of their voter registration process[68]. This type of information is used widely in Africa and Latin America as a form of identification[69].

A prime example of how personal data could be used for nefarious purposes is a hacking case involving multiple Latin American countries, where a database of email addresses was stolen and then used to spam the accounts with disinformation about a rival candidate[70]. Additionally, knowing enough personal data about someone could result in impersonation, enabling the attacker to change that specific entry in the voter registration database[71] or manipulate the vote by changing the address for vote by mail[72]. Another scenario would focus on the availability of the data on the day of election which would determine if people could vote. If such an attack is carried out against a high number of people – effectively barring them from the election – and becomes public, it also leads to an erosion of trust in the legitimacy of the election.

Personal data is not necessarily public but might end up being published and made available by the individual themself (self-reporting), government or private companies. For example, certain US states, such as Florida[73], allow access to personal data of their citizens and in Germany companies can

65 Max Biederbeck, Chris Köver, Dirk Peitz, German Angstwahl: Die digitale Nervosität der deutschen Parteien.

66 International IDEA, ICTS in Elections Database.

67 Ongoing research, International IDEA, ICTS in Elections Database.

68 International IDEA, ICTS in Elections Database.

69 International IDEA, ICTS in Elections Database.

70 Tim Maurer and Agustin Rossi, Why Latin America Needs to Prepare Now for Election Meddling.

71 Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections.

72 Minister des Innern und für Sport Hessen, Unique incidents in Hessen, Germany.

73 However, under section 97.0585, Florida Statutes, information such as a voter registration applicant's or voter's social security number, Florida driver's license number or Florida identification card number are exempt from public records disclosure. This is information under section 1.3 category of government issued data.

access this data to an extent legally via Germany's registration offices[74]. The integrity of personal data is important when its manipulation would lead to exclusion from the voting process. Availability does not seem to be part of the election hacking tactics whereas confidentiality is undermined per se by the wide accessibility of this information.

Self-Reported Data

Self-reported data distinguishes from personal data in the way that a citizen reports this information about themselves or that it is information a company derives about a user from their behavior online. It does not need to be factual or proven and/or always identifies a specific individual which also distinguishes it from like personal data. This includes biographies on social media and public messages, personality traits and opinions based on social media activity or purchasing habits[75], as well as user behavior and tracking. Parties also internally ask for self-reported personal data. The German party Liberal Democrats created a tool to ask for feedback from its party members on a specific subject[76]. Another way parties use self-reported personal can be seen in the case of the Christian Democratic party, which collected data via the app Connect17 to get insights into its potential voter base in 2017[77]. Self-reported data is essentially user-generated content and user data gleaned by companies e.g. from online behavior tracking that is used to profile audiences.

Access to these profiles/audiences is then sold to political advertisers who use it to try and shape public opinion and voter behavior. The data can however also be abused by malicious actors to distort public perception and voter behaviour, as seen in the US[78] and EU[79] context, particularly exploiting polarization and differences in the country's population. Moreover, if those tools are used by political parties/politicians in order to understand their

74 Datenschutzbeauftragter-info, Meldedaten: Wie der Staat mit uns Geld macht.

75 Those deductions might not necessarily be correct as they rely on algorithms that make conclusions about a person's behavior which might be wrong. Apart from algorithms not working well, the base data could be outdated, inconclusive or intentionally incorrect.

76 FDP Bundespartei, Meine Freiheit.

77 Christlich Demokratische Union Deutschlands (CDU), Connect 17 App.

78 Facebook, Case Study: Reaching Voters with Facebook Ads (Vote No on 8) and Politico Staff, The social media ads Russia wanted Americans to see and Adam Entous, Craig Timberg and Elizabeth Dwoskin, Russian Operatives used Facebook to Exploit racial and religious divisions.

79 Kaan Sahin, Germany Confronts Russian Hybrid Warfare and Tim Maurer and Agustin Rossi, Why Latin America Needs to Prepare Now for Election Meddling

constituency better (e.g. polls on Instagram, internal polls etc.), the integrity of that data is important as it may be used in political decision-making and to build a political strategy[80].

Self-reported data is only partially public, e.g. certain parts of social media profiles. The vast majority of data for example held by Facebook is not public (user tracking across the web, geolocation information, phone call and text activities[81]) and access to the analytics of this data is sold to advertisers. Self-reported data held mostly by private companies in the area of marketing and social media and to some extent by public pollsters. It is accessible via the companies' marketing tools or can be bought via data broker companies that receive and buy data from a range of companies and sell them[82].

Due to the wide accessibility and self-reporting nature, availability is not a problem, since it can be largely reproduced by the self-reporting individual. Integrity of self-reported data can be crucial however. If for example self-reported data such as messages on public-facing social media is altered, it can lead to reputational and political damage. Confidentiality only becomes problematic if the self-reported data was sensitive in nature (e. g. political preferences) or was collected without the user's explicit knowledge (e. g. user tracking across the web, which can be loosely seen as user-generated data).

While attacking the integrity of self-reported data is certainly a threat scenario and becomes more consequential the more political parties or local governments rely on self-reported data for their decision-making, as of now the two serious concerns stem firstly from privacy violations through user tracking, profiling and selling access to those data, and secondly the lack of security in handling this data[83] which are a threat to the confidentiality of self-reported data. Countermeasures that need to be considered therefore and include data protection mechanisms such as data avoidance, explicit consent and access restrictions.

80 Great Battlefield Podcast, Modernizing Technology and Security at the DNC, Raffi Krikorian, Chief Technology Officer of the DNC, discusses voter information databases and the future of it (minute 26)

81 Sean Gallagher, Facebook scraped call, text message data for years from Android phones

82 FTC, USA example of companies that hold consumer data
Certain data protection laws may limit the access or use of the data.

83 Dell Cameron and Kate Conger, 2017 GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters.

Government-Issued Data

Government-issued data is information that is assigned to an individual by their own government. This could be for example the driver's license ID, a specific voter identification number, social security numbers, tax identification number, passport or citizen ID number. In the voting context, this information is used mainly for the identification and authentication of a voter in the registration or voting process. Voter registration is digitized for example in the US. There are different voter ID and registration laws in the US. Some states do not require any ID, for example California. In other states, for example Alabama, a citizen must provide personal data such as name, date of birth and government issued information like a driver's license number or state ID[84] in order to register to vote. The election volunteers then use e-poll books to check off people who have voted using the databases. In other countries, voters are identified via their physical passport, as is the case in Germany. In Estonia, the government issues ID-cards to every citizen. They have two functionalities: authentication and a digital signature. Citizens can use these eID cards to vote online. Around 30% of participating voters vote online during the advanced voting phase [85].

Government-issued data is generally not public. However, it is not only accessible by the individual and the corresponding government agencies but, depending on the use case, also by the private sector entities such as tax companies, private prisons, hotels and even fitness studios[86]. Therefore, the fewer use cases the government-issued data that is used for voting and voter authentication has, the less widely shared it will be. This number in combination with other data types, such as personal data or security data, can be used to steal an identity, forge a vote or by gaining access to the database and changing for example the address of a voter. The possibility and cost of this act was studied[87]. Government-issued data needs to be available, valid and kept as confidential as possible – therefore all three *Schutzziele* apply here.

84 Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections.

85 E-Estonia, i-voting in Estonia; Valimized, statistics about Internet Voting in Estonia.

86 Michael Link, Kommentar: Unerlaubte Ausweiskopien – niemanden kümmert's.

87 Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections.

Personal Communication Data

Personal communication data is information known by at least two individuals within or outside of a group (party, campaign team, business). It is meant to stay between those stakeholders and is therefore by definition not public. If said information would become public, it would likely result in harming the reputation, status or integrity, or hurt the individual or group in some form. The concrete threat here is that personal communications are revealed that are embarrassing or otherwise harmful for example to a candidate or campaign or appear as if the information security of election related IT infrastructure, including party and campaigning systems, has been compromised. 2016 personal communication data was leaked, which revealed that Democratic National Committee members appeared to be supporting Hillary Clinton's campaign behind the scenes and mocking the campaign of Vermont Senator Bernie Sanders[88]. This ultimately led to the resignation of the DNC Chairwoman.

Even though personal communication data is supposed to be private, more than just the stakeholders involved may have legitimate access to it. For example, employees of services such as social media networks like Twitter are technically able to access direct messages exchanged between two parties[89]. The same goes for text messages, emails and so on if they are not encrypted. Additionally, this data might also be stored on systems of agencies that create campaigns for politicians[90]. Tampering with the availability and integrity of personal communication data might be problematic, but the real threat is the loss of confidentiality.

Security Data

Security data is information that is used to secure systems, such as the login for a laptop, the keyphrase for a smartphone, the account name and password for social media and email accounts, and even a password for the voting machine as well as user credentials for administrator accounts governing the entire campaign infrastructure or technical blueprints and configurations. Even a phone number could fall into this category when it is used for

88 Michael D. Shear and Matthew Rosenberg, Released Emails Suggest the D.N.C. Derided the Sanders Campaign.

89 Catherine Shu, Twitter hits back again at claims that its employees monitor direct messages.

90 Julia Löhr, Warum Jung von Matt Wahlkampf für die CDU macht.

two-factor authentification[91]. During the electoral process, username and password information is most commonly used for social media. Politicians will hand out this type of security information to staff, so they can access the social media accounts such as Instagram or Twitter. In 2017 passwords for social media were stolen, and thus hackers could access Twitter accounts of British Members of Parliament[92].

If attackers are able to take over email accounts or social media accounts, they would be able to access and manipulate other data, for example confidential data, and spread disinformation that damage the reputation of candidates and campaigns. Attackers could also conduct reconnaissance and simply monitor communications or impersonate the account holder to compromise additional systems and accounts. Another example for security data in the electoral process is that in some states a password and username combination is also required to access voting machines. With that information an attacker could change the database. That means that someone could copy the voting database to a separate machine, edit the votes, and put it back[93] or render the voting machines inoperable, undermining the legitimacy and public perception of the election.

Security data is by definition and should always remain non-public[94]. Ideally, it is not shared with a single person who is not the account holder. Most instances that require security data have a reset function, so availability and integrity are not a major challenge. Protecting the confidentiality of security data, however, is of utmost importance.

91 Wikipedia contributors. "Multi-factor authentication."

92 Press Association, Russian hackers 'traded stolen passwords of British MPs and public servants'.

93 Sam Thielman, Voting machine password hacks as easy as 'abcde', details Virginia state report and Jeremy Epstein, The Worst Voting Machine in America - Its password? “Admin.”

94 Exemption being two-factor authentification identifiers such as the email address or phone number. In those cases, it is sufficient if the first factor remains non-public. Ideally however, both factors should be non-public.

Data Type	Purpose for Elections	Accessibility	*Schutzziel*
Publicly Accessible Electoral Data	Drawing electoral boundaries and providing information about political stakeholders and the election.	Public	Availability Integrity
Personal Data	Voter authentication, registration and voting	Public *Accessible by a wide range of public and private entities.*	Integrity Availability
Self-Reported Data	Campaigning and political polling	Partially public *Voluntarily shared with private sector entities and potentially widely shared by them as well.*	Integrity Confidentiality
Government-Issued Data	Voter identification and authentication for voting	Partially public *Shared with designated government counterparts and widely with private sector entities.*	Confidentiality Integrity Availability
Personal Communication Data	Campaigning	Not public *Designated recipients and service providers only.*	Confidentiality
Security Data	Campaigning and voting	Not public *Account holder/s and possibly private sector provider of those accounts.*	Confidentiality

Table 2. Data Types

5. Conclusion

The interference of the US presidential elections 2016 was a wake-up call and several research and analysis activities have already been conducted as a response[95]. It requires us to reconsider how we think about securing the electoral process in an increasingly digitized environment. For this analysis, we focused on one of the pillars of digitalization which is the underlying data. Considering the identified election hacking tactics and possible exploitation methods of election-related data, we conclude that to properly secure the electoral process, the confidentiality, integrity and availability of data require further attention.

Though their exploitation may have lasting effects, the integrity can be restored with the right tools, similar to their availability. With the confidentiality of data, the situation is even trickier. Once its has been compromised, for example private communications have been published on the Internet, a data's confidentiality cannot be restored. Considering that an attacker might at some point be successful in overcoming security mechanisms, that the strategic motivations show that even an unsuccessful operation can still cause severe damage to the electoral process[96], and that confidentiality cannot be restored, this paper suggests to not only look at recommendations that increase security of data, such as minimum IT security standards for election IT infrastructures, but also focus on resilience through measures that mitigate the impact of a successful attack against the data driven electoral process.

95 See for example Emefa Addo Agawu, How to Think About Election Cybersecurity: A Guide for Policymakers.

96 Even if the attack is not successful, it might still be a threat to the electoral process. As shown earlier a failed attempt to for example manipulate the votes might, if it becomes public, still erode trust in the democratic process.
The Grugq, Campaign Information Security In Theory and Practice.

Election Security Recommendations and Good Practices

The list of good practices in the footnotes show examples of implementation of the recommendations in different countries[97].

I. Foundations for effective implementation of election security

Governments should...

1. define nationally what “election interference” & “systems in the electoral process” mean and treat election security as an ongoing process and practice.
2. make election security a national security priority (consider as part of domestic and foreign security). Election security should become part of the discussion among and in the same environment as other security challenges[98].
3. enable election security as a public-private-civil partnership goal. Effective election security can only be achieved through a consolidated effort[99].
4. dedicate resources for the effective implementation of election security that enables all involved stakeholders. Election security implementation needs an increased investment of financial and human resources.[100]
5. encourage and make any relevant stakeholder in the election process[101]

97 The authors are interested to hear about other examples and expand this list systematically in the future. The examples should be seen as inspirations for government looking to implement a recommendation.

98 Examples:
Dustin Volz, Patricia Zengerle, Inability to audit U.S. elections a 'national security concern': Homeland Chief
Eric Brattberg and Tim Maurer, 2018 How Sweden Is Preparing For Russia to Hack its Election.

99 Reasons for this recommendation: The private sector is involved in the supply chain of e.g. voting machines, software etc., the government is responsible for cyber defense, civil society has trusted actors and security expertise - only a coordinated approach can be effective for election security

100 Examples:
Eric Brattberg and Tim Maurer, 2018 How Sweden Is Preparing For Russia to Hack its Election
The Times staff, 2018 Illinois finalizes its plans to prevent another hack
Morgan Chalfant, 2018 Senators introduce election security amendment to defense bill.

101 Robby Mook Matt Rhoades Eric Rosenbach, 2017 Cybersecurity Campaign Playbook.

aware of security culture[102] in campaigns, parties, election offices.

II. Organization of election security

Governments should...

1. implement a permanent governmental (vertical/horizontal) coordination and exchange on protecting elections[103].
2. enact a joint mixed (governmental and non-governmental) task force for information-sharing, development of best practices and coordination of efforts across society[104].
3. identify trusted domestic actor(s) which can in cooperation with private sector, academia and civil society communicate publicly about perceived and current (!) threats[105].

102 Chris Bing, DNC pushes employees, campaigns to embrace email security habits ahead of midterms cites Raffi Krikorian, Chief Technology Officer at DNC: "Making the party secure and getting over the wounds of the hack of '16 is a cultural issue," he said. At the end of the day, "you can have the best technical defenses, but the weakest link could be your people. ... So culture change is probably one of the biggest things that we need to execute on."

103 Calvin Biesecker, DHS Creates Task Force To Bolster Election Security.

104 Examples of non-governmental and governmental task forces for election security or other related tech policy issues: Brazil Superior Electoral Court Advisory Board: FGV, Brazil's Superior Electoral Court reappoints FGV director to Advisory Board on Internet and Elections: "The purpose of civil society representatives within the Court is to propose actions to contain the spread of fake news and the use of bots during the 2018 elections. The Board's responsibilities include developing research projects and studies on the electoral rules and the influence of the internet on the elections, particularly the risk of fake news and the use of bots to spread information; providing an opinion on matters submitted by the Presidency of the TSE; and proposing actions and goals to improve the rules."
Ontario Securities Commission FinTech Advisory Team: Mondovisione, OSC announces FinTech Advisory Team
IIJ Staff, OSC seeks applicants for Fintech Advisory Committee: "The FAC advises OSC LaunchPad staff on the development and challenges regarding the fintech industry. The OSC LaunchPad helps fintech businesses in matters relating to regulatory requirements."

105 International stakeholders such as OECD could help to identify such actors.
Examples of trusted actors for election security:
Mexico's initiative "Verificado 2018", Andreas Rodriguez, Verificado 2018: Using collaborative journalism to fight fake news in Mexico
Brazil Superior Electoral Court partnership with Brazil Computer Society, Angelica Mari, Brazilian government tries to prove e-voting is safe - A partnership with the Brazilian Computer Society aims at convincing the population that the electronic voting method is fraud-proof.

III. Security mechanisms that proactively secure election infrastructure

Governments should ...

1. establish and conduct a continuous risk management process for technologies that are used in elections. This process should ensure that new and old electoral systems comply and stay current with state-of-the-art IT-security practices. Implement a national *hack the elections program* for finding vulnerabilities in hardware, software and online services used for elections and campaigning and include an obligation to fix them[106].
2. ensure that there are mechanisms in place[107] that monitor, detect and warn against cyber attacks on elections infrastructure and integrate them into existing security practices or threat analysis done for other security challenges[108].
3. adopt a strategy to secure the election infrastructure cyber security supply chain[109] which includes software, hardware and online service which are used in the electoral process. This strategy should comprise features

106 Good practices for risk management processes:
DefCon Hack The Voting Machines Village, Matt Blaze et al, DEFCON 25 Voting Machine Hacking Village Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure
NIST standards for voting systems, NIST, Voluntary Voting System Guidelines (VVSG) Recommendations to the EAC, August 31, 2007
BSI Germany technical standards, Federal Office for Information Security Germany, Technical Guidelines.

107 In case this is not an option due to resources ensure that information level about cyber attacks on election infrastructure can be accessed from another country.

108 Example of threat analysis centers that adopted monitoring for election security, Federal Office for Information Security, IT-Lagezentrum
Example of intelligence sharing about election security threats, Greenberg, The NSA confirms it: Russia hacked french election infrastructure.

109 Wikipedia contributors, Supply chain cyber security.

such as security standards, report mechanisms and certification schemes[110].

4. require companies that handle (large amounts of) citizen/voter data, such as social media companies, to apply data minimization as a security principle for processing election-related data[111].
5. require an auditable trail for the voting process, ensure a secure, transparent and accountable voting process. Foster respective research through government funding.
6. develop election security processes and preparation for worst cases, e. g. identifying threat scenarios and through scenario exercises educate operational and strategic audiences who are relevant to the election process[112].

IV. Capacity building and training about election security for key stakeholders and the public

Governments should...

1. implement and encourage capacity building measures and access to technical expertise for campaigns, politicians, parties and spouses of high ranking politicians provided by the public and private sector and civil society organisations. Capacity building can be through technical expertise by for example there could be vetted IT volunteers or in form of funding that ensures security to those vulnerable stakeholders[113].

110 Moreover, if this process was harmonized among countries and adheres to a high standard the quality assurance along the whole supply chain is better. International supply chain security initiatives already exist but would need to be adopted for cyber security of elections.
Example approaches countries have taken for supply chain cyber security:
UK's National Cyber Security Center principles on supply chain security, NCSC, Guidance The principles of supply chain security
United States, Department of Homeland Security National Strategy for Global Supply Chain Security Germany's research for Civil Security Securing the Supply Chain, Federal Ministry of Education and Research, Research for Civil Security Securing the Supply Chains.

111 In accordance with this paper.

112 Example: Swedish Civil Contingencies Agency (MSB), Jill Bederoff, Sweden is warned about foreign interference ahead of its election – and the country has 2 priorities to ward off attacks.

113 Examples:
An idea that could be adopted for election security volunteers, BSI Certified IT Pen Testers, Federal Office for Information Security, Zertifizierung als Penetrationstester
Security checklist and data boot camp by DNC, Chris Bing, DNC pushes employees, campaigns to embrace email security habits ahead of midterms.

2. ensure critical consumption of news online and offline[114], especially in the context of elections and the adversarial geopolitical environment, through making it an essential subject in curricula along with civic education and create a specific curriculum for this recommendation taking into consideration best practices from Estonia[115], Finland[116] and Italy[117].

V. Strategic communications to create resilience

Governments should...
Conduct proactive strategic communication toward media and voters about the structure and security of the voting process and IT infrastructure should be ensured to increase trust in the electoral process. Goal is to dispel wrongful perceptions, reduce fear, improve transparency and do the opposite of *security-by-obscurity* -- provide this information regularly for example at voter registration (US) or voter announcement mail (Germany), and other opportunities as practical.

VI. Leveraging the potential of International Cooperation on Election Security

Governments should...
1. make sure that election security related threat information is shared with intelligence partners/ allied countries[118].
2. support and promote efforts to create and maintain a publicly available database of international collection of best practices on how to secu-

114 More should also be done for critical (local) journalism and journalists in terms of funding and education. This is not part of the scope of this paper but could assist to combat (hybrid) threats.

115 Example: Estonia ranks among the "best-equipped countries to resist the post-truth, fake news and their ramifications", Open Society Institute Sofia, Common Sense Wanted: Resilience to 'Post-Truth' and its Predictors in the new Media Literacy Index 2018.

116 Example: Finnish Media Education, National Audiovisual Institute, Finnish Media Education Promoting Media and Information Literacy in Finland.

117 Example: Italy's Curriculum, NPR, Italy Takes Aim At Fake News With New Curriculum For High School Students; Jason Horowitz, In Italian Schools, Reading, Writing and Recognizing Fake News.

118 Example: "Establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.", G7, CHARLEVOIX COMMITMENT ON DEFENDING DEMOCRACY FROM FOREIGN THREATS.

re the electoral process, including their individual implementations and (positive and negative) implications[119].

3. establish international standards for secure voting technologies.
4. include international standards on election security and best practices into current capacity building schemes as part of international development efforts.

119 Examples of international networks where best practices are already shared collected by Brazil Superior Election Court, Cooperation with International Organizations.

Acknowledgement

This analysis has been supported by members of the Transatlantic Cyber Forum through online collaboration and joint workshops in Washington D. C. and Berlin. The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the working group members or that of their respective employer/s. Acknowledging essential contributions of:

1. Emefa Addo Agawu, New America
2. Geysha Gonzalez, Eurasia Center, Atlantic Council
3. Joseph Lorenzo Hall, Center for Democracy & Technology
4. Stefan Heumann, Stiftung Neue Verantwortung
5. James Lewis, Center for Strategic and International Studies, Washington
6. Marco Macori, Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences
7. Nemanja Malisevic, Microsoft
8. Tim Maurer, Carnegie Endowment for International Peace
9. Igor Mikolic-Torreira, RAND Corporation
10. Thomas Reinhold, Institute for Peace Research and Security Policy Hamburg/ cyber-peace.org
11. Laura Rosenberger, Alliance for Securing Democracy, The German Marshall Fund of the United States
12. Bruce Schneier, Harvard Kennedy School
13. Isabel Skierka, Digital Society Institute at ESMT Berlin

Annex A: Attack Vectors

An attack vector is a path or route used by an adversary to gain access to a target's system[120] and therefore forms the basis for any election hacking tactic. Outlined below is a broad overview of the most common attack vectors threat actors use to reach their objective.

Exploiting Software Vulnerabilities
Electronic devices run software, be it a personal smartphone or a server that hosts an online service, such as email accounts or social media platforms. Software, especially the more complex the underlying code gets, has vulnerabilities. A software vulnerability is a security flaw, glitch, or weakness in the software which can create a opening for a threat actor to exploit[121]. A threat actor typically does this by creating malicious code which exploits the vulnerability that can then give the threat actor access to the target. Software vulnerabilities are mostly inconspicuous to users which makes this an ideal covert attack method. Most of the attack vectors below to a certain degree rely on existing vulnerabilities to be effective. Vulnerabilities can be exploited remotely or locally, for example by connecting an infected USB device to the target machine.

Supply Chain Attack
A supply chain attack is also a credible election hacking tactics for attacking elections[122]. In this case it would mean that the adversary would try to compromise the systems of the vendor, for example of voting machines, and infect the software updates. When those updates are rolled out to the voting machines in the field, they would be compromised. The infected voting machines could then grant the attacker access, show altered results or be dysfunctional in any possible way.

Spear Phishing
This fraudulent attack is one where the threat actor tries to deceive his/ her target into believing the content presented comes from a trusted source. Depending on the use case, this "trusted source" which is being mimicked by the threat actor might be an email service provider, a co-worker, a friend or an institution, claiming for example to be sending a new policy paper about

120 ISACA, Attack Vector Definition, 2018.

121 Oscar Celestino Angelo Abendan II, Gateways to Infection: Exploiting Software Vulnerabilities.

122 Institute for Critical Infrastructure Technology, The Painfully Vulnerable Election System and Rampant Security Theater.

a recent event. The overall goal is to gain access to the target's system or the target's accounts, such as email or corporate infrastructure, when the target unknowingly hands over account information to the threat actor; this can also be accomplished by infecting the target's computer with malicious code, or a virus which compromises the security of the system[123]. A common method of spear phishing is to use email to deliver links, typically to navigate the target to websites controlled by the threat actor, or malicious attachments, are presented to the target to click on.

Insider Threat
Insider threat refers to the danger that malicious actors can pose if they are work inside an institution (including past employees whose credentials have not been revoked and third party contractors) -- or its supply chain. An insider may have direct access to important files, know security protocols or might, in the worst case, be equipped with administrator privileges for the entire IT infrastructure. Their access and the ability to cover their tracks causes a huge potential for sustained damage[124].

Whaling
Is a more targeted type of spear phishing by which the same techniques are used, but focuses on high value targets such as business executives, politicians, and high ranking government officials. The highly personalized nature of these attacks make them more difficult to detect[125].

Waterholing
This attack begins with the threat actor carefully conducting reconnaissance on a target's organization to see what websites are frequently visited. After this is identified, the attacker will try to compromise such websites first and then insert an exploit into them. This then allows the attacker to infect a targets computer when it visits the website[126].

Social Engineering
Social engineering attacks typically involve some form of psychological manipulation of the target. An often-used tactic in social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading it to promptly reveal sensitive information such as

123 Faris Azimullah and Anu Nayar, Spear Phishing 101: What is it and how to avoid it?

124 Marcell Gogan, Insider Threats as the Main Security Threat in 2017.

125 Nena Giandomenico, What is a whaling attack? Defining and Identifying whaling attacks.

126 Oscar Celestino Angelo Abendan ll, Watering hole 101.

passwords, click a malicious link, or open a malicious file[127]. The recent proliferation of fake news on social media platforms geared towards highlighting divisive issues underlines the effectiveness of this attack[128].

Spoofing
A spoofing attack is when a malicious party impersonates another device or user on a network in order to bypass security measures or deceive a target[129]. Spoofing is not only a technical type of an attack but can also be used in social engineering strategy. For example, a threat actor typically modifies a website, email address, or online persona to look similar to a trusted source in order to deceive their targets.

Man-in-the-Middle [MITM]
This attack method has the threat actor focus on becoming a pass through mechanism between a user and the server or application the user tries to access. For example, one common employment of this attack method is by compromising an unsecured or weakly secured router which is used e. g. for wifi in a coffee shop or airport. Once the threat actor takes over the router, they can monitor the activity of a users who are connected[130] and alter the content of communications and deliver malware to the target's computer, potentially compromising it for later use by the attacker[131].

(Distributed) Denial-of-Service [DDoS]
A (distributed) denial-of-service attack is an attack method where a threat actor coordinates multiple requests to a website or online service which overwhelms it causing it to be unavailable for access[132]. In other words, denying users information or the capability that a website, service or platform offers.

127 Nate Lord, Social engineering attacks: Common techniques & how to prevent an attack.

128 Kerry Tomlinson, Fake News can Poison your Computer as well as your Mind.

129 Veracode, Spoofing attack: IP, DNS & ARP.

130 Symantec, What is a man in the middle attack?

131 Serge Malenkovich, Was ist eine Man-in-the-Middle-Attacke?

132 Akamai, (Distributed) denial-of-service Attack.

Über die Stiftung Neue Verantwortung

About us

The Transatlantic Cyber Forum (TCF) has been established by the Berlin based think tank Stiftung Neue Verantwortung (SNV). The SNV is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state.

The Transatlantic Cyber Forum is a network of cyber security experts and practitioners from civil society, academia and private sector. It was made possible with the financial support from the Robert Bosch Stiftung and the William and Flora Hewlett Foundation.

About the Authors

Sven Herpig is the project director of the Transatlantic Cyber Forum (TCF), bringing together American, German and other EU-experts to collaborate on cyber security policies.

Julia Schuetze works as project manager of the "Transatlantic Cyber Forum“. Her research focus is on cyber operations against electoral processes, comparative cybersecurity policy and multi-stakeholder models.

How to Contact the Authors

Dr. Sven Herpig
Project Director International Cyber Security Policy
sherpig@stiftung-nv.de
+49 (0)30 81 45 03 78 91

Julia Schuetze, M.A.
Project Manager Transatlantic Cyber Forum
jschuetze@stiftung-nv.de
+49 (0)30 81 45 03 78 82

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de