June 2017 | Sven Herpig

Cyber Operations: Defending Political IT-Infrastructures

A comparative problem analysis supported by the Transatlantic Cyber Forum

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Die vorliegende Analyse beschäftigt sich mit der Reaktion auf Cyber-Operationen gegen politische IT-Infrastrukturen. Basis hierfür formen die Fallstudien zu den Angriffen gegen das Democratic National Committee (USA) und den Bundestag (DEU). Zentrale Elemente der Analyse sind das Verhältnis zwischen verschiedenen Akteuren innerhalb und außerhalb der Cyber-Sicherheitsarchitektur, die Zurechenbarkeit von Cyber-Operationen, sowie die Effektivität bisheriger Reaktionen.

Die zugrundeliegende Hypothese ist, dass Deutschland und die Vereinigten Staaten Elemente der Abschreckungstheorie ("Deterrence Theory") anpassen und anwenden sollten, um zukünftige (erfolgreiche) Cyber-Operationen gegen ihre politischen IT-Infrastrukturen zu verhindern. Trotz des ambivalenten Hintergrundes der Abschreckungstheorie erscheint es sinnvoll diese für die Betrachtung des Schutzes von politischen IT-Infrastrukturen vor Cyber-Operationen wieder aufzugreifen. Die Ergebnisse welche der Arbeitsgruppe als Ausgangsbasis für die zukünftige Erarbeitung der Handlungsoptionen dienen werden sind:

1. Schutz der politischen IT-Infrastrukturen ("Deterrence-by-Denial");
2. Analyse möglicher Optionen für Gegenmaßnahmen ("Deterrence-by-Retaliation");
3. Vertrauen in internationale Beziehungen ("Deterrence-by-Norms" / "-Entanglement");
4. Analyse der Vorbedingung der Zurechenbarkeit ("Attribution").

The analysis focuses on the response to cyber operations against political IT-infrastructures. The attacks against the Democratic National Committee (US) and Parliament (GER) are the case studies used as basis for this research. Core elements of the analysis are the liaison of the relevant stakeholders inside and outside of the cyber security architecture, the attribution of cyber operations as well as the effectiveness of previous responses.

The working hypothesis is that Germany and the United States should adapt and implement different aspects outlined in deterrence theory in order to prevent future (successful) cyber operations against their political IT-infrastructures. Deterrence does have an ambivalent past but it seems to be might be prudent to revisit and adapt it not only to the cyber domain - but specifically to cyber operations against political IT-infrastructures. Those results which form the foundation for the upcoming recommendations drafted by the working group are:

1. Protecting the political IT-infrastructure ("deterrence-by-denial");
2. Assessing options for show of force ("deterrence-by-retaliation");
3. Relying on international relations ("deterrence-by-norms"/ "-entanglement");
4. Analyzing the pre-condition attribution.

Contributions

Contributions to this paper have been provided by the members of the Transatlantic Cyber Forum working group on "cyber defense & political infrastructures". These include amongst others Constance Baban (Brandenburgisches Institut für Gesellschaft und Sicherheit), Nathaniel Gleicher (Center for Strategic & International Studies/ Illumio), Stefan Heumann (Stiftung Neue Verantwortung), Johannes Klick (SCADACS), Marco Macori (Institute for Security and Safety, Technische Hochschule Brandenburg), Igor Mikolic-Torreira (RAND Corporation), Thomas Reinhold (CyberPeace), Volker Roth (Institute for Computer Science, Freie Universität Berlin), Julia Schuetze (Stiftung Neue Verantwortung), Ben Scott (New America/ Stiftung Neue Verantwortung), Isabel Skierka (Digital Society Institute, European School of Management and Technology).

Introduction

Since at least the spring of 2016, the United States and Germany are aware of a shared problem: they lack appropriate strategies regarding government responses to cyber operations[1] against their political IT-infrastructures[2]. Finding a common solution to this challenge would not only bolster national security but could also improve the transatlantic relationship where cyber issues are concerned and take lead in the international discussion.

This paper offers side by side analysis of the 2015 cyber operation against the German parliament's network and the 2016 breach of the Democratic National Committee's IT-infrastructure[3]. The two cases show that political IT-infrastructures were targeted with technically simple but effective means. In the US case, the attackers were able to access substantial amounts of sensitive emails and had access to the Democratic Congressional Campaign Committee and the main computer network of the DNC. In the German case, attackers gained full access to the entire IT-infrastructure of the German parliament.

The goal of the analysis is to identify commonalities, derive the government's main challenges and offer a hypothesis on how to effectively respond to cyber operations of this kind[4]. A comparative approach is applied to outline the attack patterns, assess the damage, depict the technical and political responses as well as review the effectiveness of those responses. These case

1 Cyber operations are defined here as the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against political IT-infrastructures in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/ or harm a targeted political unit. https://www.stiftung-nv.de/sites/default/files/antiwar_cybertriangle-herpig.pdf

2 Political IT-infrastructures are within this context understood as the IT-systems, networks, and cloud services accounts of politicians, political parties, legislatures and any other institution engaged in the conduct of elections. These stakeholders and IT-infrastructures are at the core of any political system. Other relevant stakeholders may include executive branch agencies and leaders, especially at the highest level, think tanks working in the field of national security as well as the institutions of the judiciary.

3 The scope of this case study is strictly limited to the operation against the DNC, not involving parallel events such as the attacks against the electoral process. Find more information about that operation here: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ and https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

4 Further research might widen the scope to include other related incidents such as the 'Macron-Leaks', http://time.com/4801295/russia-hacking-cyber-security-france-french-election-emmanuel-macron-apt28/

studies shall serve as building blocks for all future studies conducted by the Transatlantic Cyber Forum working group on cyber defense and political infrastructures[5].

The problem analysis goes beyond foreign intervention ("election meddling") and includes all cyber operations against political IT-infrastructures at all times. Cyber operations are considered peacetime activities[6] which inherently have political significance and possess the ability to create fear, uncertainty and doubt (in the political system). They can be part of broader intelligence operations as shown in both case studies. However, the analysis is limited strictly to the interference with IT-infrastructures used and does not encompass other means such as propaganda or information operations.

The analytical perspective evaluates the mitigation strategies of ongoing operations. But the primary purpose is to surface policy and practice for the prevention of future (successful) attacks. That is, the problem of defending political IT-infrastructure is fundamentally about avoiding damaging attacks and not generating a menu of options for remedy. However, from a technical point of view, mitigation is an important aspect to limit the impact and should therefore not entirely be discarded. Within that framework, the outcomes of the case studies suggest that revisiting deterrence theory might be a prudent starting point for further research. The conclusion of this paper therefore offers an outline of deterrence options that may serve as the structural basis for the next phase of discussion in this working group.

Cyber operation against the German Parliament

Attack pattern

The German Parliament's computer network - the 'Parlakom' - suffered from a foreign cyber operation in 2015. In April 2015, attackers sent emails with links to infected websites to the offices of several members of parliament across party lines. Several recipients opened that link, and their computers were infected with malicious software which deployed a tool for password harvesting ('mimikatz')[7]. This malware enabled the attackers to harvest cre-

5 https://www.stiftung-nv.de/en/project/international-cyber-security-policy#zweitens

6 As long as cyber operations belong to the domain of intelligence and espionage activities, they are illegal in the target state but have historically never been treated as an act of war. They do however constitute a serious crime. The Tallinn Manual only acknowledges those cyber operations where the impact rises to a level equivalent to the use of force in armed attacks. Until now, cyber operations against political IT-infrastructures have not yet had such an impact. With the United States recently declaring election systems as critical infrastructures, this might change in the future: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

7 Due to the lack of logs from the time of the initial attack - retention of logs was limited to 7 days - it is unclear who and how many recipients clicked the link to the malicious website, https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_7_20150612

The BSI is only certain about 16 office computers of members of parliament which have been compromised, https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_7_20150611

dentials from users and domain administrators, granting them full access to the entire network structure. The attackers then started to exfiltrate documents[8].

The heads of the German domestic intelligence agency (BfV) and the national cyber security agency (BSI)[9] as well as the independent security researcher Claudio Guarnieri[10] found some evidence attributing the attack to APT-28/ Sofacy Group, which is of Russian government origin. However, only the BfV was confident enough about its findings to publicly[11] link the attack to Russia, calling it highly likely that they were responsible for it.

Judging by the known targets of the attack and their individual roles within the parliament and government[12], it seems possible that this attack was not primarily aimed at collecting 'kompromat' to use in active measures. Apparently learning about political positions, for example in international negotiations, thus getting to a political vantage point and making it a cyber-enhanced 'classic' espionage operation seems a possible goal[13].

It is important to note that Germany has built a secure government network, the IVBB, that connects most federal government institutions. IVBB features enhanced security mechanisms provided by the BSI. In addition to regular security products and services, this network runs two additional protection mechanisms. One system called "Schadsoftware-Erkennungs-System" (translation: malware-detection-system) (SES) protects against targeted cyber attacks such as spear-phishing - the attack vector used in the Parlakom operation - and the other one called "Schadsoftware-Präventions-System" (translation: malware-prevention-system (SPS) protects internal devices from accessing malicious servers and websites[14]. This includes a protection against data exfiltration from infected systems through blocking connections to known malicious IP addresses outside the secured IVBB ("blacklisting").

8 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/

9 http://dip21.bundestag.de/dip21/btd/18/111/1811106.pdf

10 https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

11 http://www.faz.net/aktuell/politik/hackerangriff-auf-bundestag-verfassungsschutz-verdaechtigt-russische-dienste-13666187.html

12 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland

13 In military environments also referred to as "achieving information dominance", http://www.iwar.org.uk/iwar/resources/info-dominance/issue-paper.htm

14 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Jahresberichte/BSI-Jahresbericht_2010_pdf.pdf?__blob=publicationFile

The defenses built into this system would have prevented the Parlakom attack[15]. However, the Parliament is not connected to the IVBB because it is part of Germany's legislature and thus does not fall under the jurisdiction of the BSI, which created and operates this enhanced security mechanism. Instead of relying on the support from the BSI, the legislature, as an independent branch of government, insists on running its own IT-infrastructure. This insistence is in no small part due to the view among political parties that the security and privacy of their communications should remain outside the control of the executive branch. As one of the mitigation activities of the Parlakom attack, the Bundestag adapted some security mechanisms from the BSI for its IT-infrastructure -- though it continues to be run separately[16].

Damages

There is no official number estimating the cost associated with the fallout or the remedy to the Parlakom hack. It is known that at peak ten specialists from the BSI as well as two experts from the company BFK and one from the German Telekom (DTAG) assisted the IT-staff of the parliament in the mitigation, recovery and adoption of new security mechanisms[17]. However, the financial repercussions are of course the least of all problems when looking at damages done to political IT-infrastructures. In addition to the manpower needed to respond, Parlakom had to be taken offline for 4 days - including a weekend[18] - effectively preventing the parliament from doing their day-to-day-work. Moreover, the attackers extracted a trove of documents[19] - rumored to be 16 Gigabytes[20] - from the network before their access was denied. The damage could have been far worse as the attackers had full access to the political IT-infrastructure. So far none of the exfiltrated documents seem to have found their way into the public domain. As Germany is heading for its

15 The Bundestag was running some similar but less up-to-date and sophisticated security mechanisms. As of April 13, the IVBB was protected against the attack that penetrated the Parlakom, the Parlakom-Hack took place two weeks later, https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestags-hack-wie-man-die-abgeordneten-im-unklaren-liess/#aktenvermerk_2015060511

16 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland

17 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-2

18 https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_9_20150910

19 The network must only be used for non-classified documents or documents classified with the lowest standard "Verschlusssache - Nur für den Dienstgebrauch". Data with higher level of classification is only permitted to be handled manually (non-digital) in the parliament, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland

20 As it is unclear what kind and type of data was exfiltrated, the sheer size of exfiltrated data does not necessarily matter.

2017 federal elections, however, additional political damage might still be inflicted by publishing the documents.

Technical response

When the IT-staff of the parliament first came across suspicious behavior within its network, it informed the BSI. While a preliminary analysis was ongoing, a British company informed the BfV that it has found documents from the German parliament on its servers[21]. The BfV promptly informed the parliament, the BSI and the interagency BSI-led cyber defense center (Cyber-AZ) about those findings[22]. Lacking proper authority to protect the parliament's IT-systems, the BSI was formally asked by the parliament's information and communication technology oversight body ("IuK-Kommission") to assist in handling and mitigating the incident. Three days after it was informed by the BfV, the BSI deployed a forensics team to the Bundestag[23]. The IT-forensics specialists of the BSI teamed up with two employees from the IT company BFK which had been working with the government for some time already[24]. While the experts assessed the situation, as much traffic as possible was routed through the IVBB to make use of the special security features of this network[25]. After the analysis had been completed, the entire network was taken offline for 4 days and brought to a non-compromised state[26]. The Parlakom was equipped with some of the security features from the IVBB to protect against similar attacks in the future.

Having provided some of the initial information about the ongoing cyber operation, the BfV offered its assistance as well. The offer was rejected by the IuK-Kommission[27] but the BfV was instead allowed to consult. This means they were not allowed to access the compromised computer systems of the members of parliament, but they were permitted, for example, to provide further intelligence for the attribution of the operation[28].

---

21 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-2

22 https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestags-hack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_6_20150512

23 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-2

24 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-2

25 https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestags-hack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_6_20150512

26 https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_9_20150910

27 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-2

28 https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#aktenvermerk_20150605

The reason for the IuK-Kommission's rejection is rooted in Germany's strong privacy culture and some parliamentarians' distrust of intelligence services. Those reservations are deeply connected to Germany's past and the collective memory of almost omnipresent secret security services during the Third Reich as well as the GDR. Especially the leftists party DIE LINKE strongly refused any involvement of the domestic intelligence agency. Until 2014, members of the party, including elected members of parliament, had been on the "watchlist" of the BfV.

Political response

Apart from the internal debriefings of the government and parliament, as well as an investigation by the Federal Prosecutor's office[29], there was only two overt, external responses to the Parlakom cyber operation[30]. A representative from the Chancellery warned the Russians during his visit in Moscow[31]. Additionally, the head of the BfV publicly called-out Russia for the operation[32]. As a political response, it would fall under the 'naming and shaming' category, but it was neither issued by the chancellor nor by one of the ministers, though likely with the administration's blessing. The BfV is an agency under the Ministry of Interior and not under the Chancellery, the Ministry of Defense or the Federal Foreign Office. Therefore, the message was more likely directed at the German public for domestic political reasons, and only secondarily towards Russia. Though it should be assumed that the message was intended to reach Russia as well.

29 The investigation started in January 2016 - 8 months after the operation became public. At this time it has not yet been concluded, https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_7_20150611

30 There has been an internal meeting between Chancellery, foreign and domestic intelligence agencies, Federal Foreign Office, Ministry of Interior and the Ministry of Defense in January 2016 which tasked the intelligence agencies to draft a report analyzing the cyber operation and its political framework. The report never got published, not even in an unclassified version. The only direct outcome of the dossier is the decision of the Federal Security Council to assess the possibility of digital retaliatory/ counter strikes, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-5

Chancellor Merkel also raised the issue directly with President Putin during a recent visit to Russia, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-6

31 http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/seite-5

32 http://www.handelsblatt.com/politik/deutschland/cyberattacke-auf-den-bundestag-geheimdienst-von-russischer-schuld-ueberzeugt/13594038.html

Effectiveness of the response

Since the 2015 cyber operation against Parlakom, there have been additional cyber operations against the parliament and several political parties[33]. Evidence gathered during those operations points again to APT28, hence Russia[34]. The attack pattern seemed very similar to the one in 2015. In early 2017, there was another incident with the parliament's infrastructure[35] which was later revealed to be just a regular drive-by-attack from an unknown source launched from a compromised Israeli newspaper website. The fact that those attacks were not successful might be attributed to the lessons-learned and security mechanisms adopted after the 2015 incident. The technical response seems to be effective. The fact that several political stakeholders were attacked again in 2016 by similar means, however, reflects a certain failure of the political response as it did not deter future attacks - from the allegedly same attacker.

Conclusion

With German federal elections coming up in September 2017, politicians are becoming increasingly worried about another cyber operation or delayed repercussions from the 2015 attack. Rightfully so, because not only are the documents extracted in the 2015 operation still out and could resurface, moreover the 2016 operations also show that deterrence through political response - if the BfV's Russian attribution statement and the diplomatic message are seen as that - has failed. This increases the likelihood of another operation. Even though the BSI started offering assistance to parties and parliament in the pre-election period[36], it is not responsible for their protection. In fact, they are completely responsible for their own IT-infrastructure with no regulations or minimum standards to hold them accountable to. This security weakness - rooted partially in political mistrust between parts of the Parliament and the executive - remains despite the experience of the Parlakom breach, subsequent attacks, and the absence of any meaningful deterrence strategy.

33 http://dip21.bundestag.de/dip21/btd/18/107/1810759.pdf

34 http://dip21.bundestag.de/dip21/btd/18/107/1810759.pdf

35 http://www.sueddeutsche.de/digital/netz-sicherheit-hackeran-griff-auf-den-bundestag-1.3440215

36 http://www.spiegel.de/netzwelt/netzpolitik/bundestagswahl-2017-bsi-chef-arne-schoenbohm-warnt-parteien-vor-hacker-angriffen-a-1136542.html

Cyber Operation against the Democratic National Committee

Attack pattern

Two cyber operations[37] were independently carried out against the DNC allegedly backed by the same state in 2015/ 2016[38]. The first cyber operation breached the DNC IT-infrastructure in July 2015. A spearphishing campaign launched in March 2016 led to another breach[39]. In both cases, email accounts of members of the Democratic Party were targeted for credential theft, which was then used to access e-mails and the political IT-infrastructures of both the Democratic Congressional Campaign Committee and the DNC. The attackers were able to maintain access and monitor communications until June 2016, exfiltrating a large volume of documents and emails.

During the first cyber operation in 2015, the UK faced a similar yet unsuccessful attack[40]. The GCHQ was able to thwart the cyber operation targeting the British general election, presumed to originate from the Russian group Fancy Bear/APT28/Sofacy. British intelligence then tipped-off the CIA when it learned that a similar attack was being carried out against the US. Learning about the possible cyber operation against the DNC, the FBI tried to alert the DNC of the breach in autumn 2015. However, the responsible DNC contractor apparently did not take the warning seriously. It took several attempts and weeks before the DNC contact believed in the authenticity of the FBI alert. Even after meeting in person with an FBI agent, the contractor remained skeptical about the issue.[41] The FBI, for their part, did not reach out to other individuals at higher levels within the DNC to alert them about the suspected attack. Considering the role of the DNC, especially during presidential elections, and the proximity of the responsible FBI office to the DNC headquarters, this pattern seems quite remarkable and raises important questions about the FBI's approach.of mishandling raises critical questions about the FBI's approach.

When the DNC was finally convinced about the authenticity of the FBI alert in March/April 2016, they hired the private IT-security company Crowdstrike to analyze the networks and assess the damage. By that time, the DNC had already been breached by a second cyber operation. Two months later[42], Crowdstrike released a corresponding technical report and made a preliminary attribution for the attack.

---

37 According to former FBI director Comey, there were hundreds of operations carried out against American entities during that time, https://www.nytimes.com/video/us/politics/100000005151437/james-comey-live-hearing.html

38 Timeline according to CNN, http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/

39 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

40 https://www.independent.co.uk/news/uk/politics/uk-general-election-russia-hacked-cyber-attack-a7580076.html

41 https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

42 It is not entirely clear what happened in the months between FBI notification and the Crowdstrike involvement.

Starting in June, the extracted data was publicly released by a virtual persona calling itself "Guccifer 2.0"[43], on the anti-secrecy platform WikiLeaks as well as DCLeaks.com. Some of the information was also exclusively made available to media outlets. None of the analyzed documents was found to be a forgery so far. In July, technical details of the cyber operation (command-and-control structure and SSL certificate) were found by Thomas Rid[44] to be congruent with those in the attack against the German parliament.

Damages

Among the data extracted from the DNC IT-infrastructure was email correspondence to and from the DNC staff and leadership. Leading up to the Democratic National Convention, 19,252 emails and 8,034 attachments from the exfiltrated data were posted on WikiLeaks. The published emails came from leading figures in the DNC campaign dated from January 2015 to May 2016[45]. The emails revealed that the DNC tried to undermine the candidacy of Senator Sanders, leading to the resignation of DNC Chair Wasserman Schultz on the eve of the Convention[46]. Many observers have suggested that the appearance of impropriety within the Democratic Party revealed by these data dumps may have been one of the contributing factors to President Trump's election victory. In the midst of this public embarrassment, the DNC was also without its IT-infrastructure for a weekend in May in order to restore security. Similar to the cyber operation against the German parliament, the exact financial damage is unknown. But it is certainly dwarfed by the political cost (i. e. impact on the elections) of the scandals that followed the hack.

Technical response

Both the DNC and the RNC implemented their IT-infrastructures for the 2016 election with clear knowledge that cyber attacks were highly likely. Yet they did not dedicate resources to security commensurate with this threat, nor did they benefit from the assistance of government security agencies. Neither the NSA, which handles federal information assurance, nor any other agency is responsible for providing information security to the political parties.

---

43 Journalists from the Motherboard platform chatted up the person behind the Guccifer 2.0 persona who claimed to be a lone hacker from Romania. Their finding was that this person was unlikely to be Romanian as he/ she was not able to reply in coherent Romanian. Over the next few months, the persona made additional false claims about its supposedly Russian identity. The full chat is available here: https://motherboard.vice.com/en_us/article/dnc-hacker-guccifer-20-full-interview-transcript

44 https://twitter.com/RidT/status/751325844002529280

45 https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/

46 https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Only in April 2016 did the DNC eventually acknowledge that something suspicious was going on in their IT-infrastructure. In response, they contracted a specialized IT-security company called CrowdStrike. CrowdStrike immediately deployed its incident response group to tackle the suspected breach[47]. The technical details of the attack were found to match those from two groups previously known for carrying out several other cyber operations, inter alia against the German parliament: Cozy Bear (APT29) and Fancy Bear (APT28 / Sofacy)[48]. After the preliminary findings and attribution, the DNC hired two additional IT-security companies Mandiant and Fidelis Cybersecurity. These two independently corroborated CrowdStrike's assessment[49]. CrowdStrike stayed on the case in order to prevent the attackers from regaining access to the DNC IT-infrastructure.

Political response[50]

The FBI launched an investigation into the breach which ultimately became public in July 2016. In June, when first information about the breach surfaced in the media, CrowdStrike released its assessment officially accusing Russia of being behind the cyber operation[51]. President Obama then formally accused Russia of meddling in the presidential elections on October 7. A DNI-led joint report[52] confirmed evidence pointing towards Russian origin of the DNC cyber operations - as well as the attack later directed against Clinton campaign chairman John Podesta. The (public) failure of the DNI report is partially based on an attributional claim that did not provide clear evidence and sowed skepticism in the expert community. The independent security researcher who was already analyzing the cyber operation against the German parliament concluded on the matter of attribution: "All in all, technical circumstantial attribution is acceptable only so far as it is to explain an attack. It most definitely isn't for the political repercussions that we're observing now. For that, only documental evidence that is verifiable or intercepts of Russian officials would be convincing enough, I suspect"[53].

47 The company used its Falcon Platform to analyze the systems and networks and found traces of two cyber operations, https://www.crowdstrike.com/resources/data-sheets/crowdstrike-falcon-platform-data-sheet/

48 https://www.wired.co.uk/article/dnc-hack-proof-russia-democrats

49 https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html

50 An overview over the development of the political response can be found here: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/

51 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

52 It was only published in an unclassified version which did not include compelling evidence, https://www.dni.gov/files/documents/ICA_2017_01.pdf

53 https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/

Several members of Congress and the Clinton campaign publicly "named and shamed" Russia for the cyber operation. Senator McCain even went on record saying that those operations were an act of war conducted by Russia[54]. After talking to Putin directly, President Obama implemented a series of responses through an executive order on December 29, 2016[55]. The president enacted economic sanctions on Russian intelligences agencies, the expulsion of 35 Russian diplomats - believed to be intelligence agents - and the shuttering of two compounds which allegedly served as locations for Russian espionage activities. Covert operations - namely the deployment of "implants" into Russian IT-infrastructures - were designed and authorized by President Obama but did not reach operational status within his term[56]. In January 2017, the Department of Homeland Security (DHS) declared election infrastructure as critical infrastructures[57].

In terms of severity of response, James Lewis from CSIS states that this is 'the biggest retaliatory move against Russian espionage since the Cold War'. Meanwhile, US Senators McCain and Graham called it 'a small price to pay' compared to the gravity of the crime. Political response consisted of foreign policy tools, namely economic and diplomatic sanctions. However, the tension between policy and politics (which we also saw in the German case) were once again highly significant. Cooperation between political parties and law enforcement was poor, and the policy responses were delayed and contorted by concerns over how an active cyber-conflict with Russia would impact ongoing US election campaigns. The American post-election politics towards Russia are another reason why the impact of the response has not been substantial.

Effectiveness of the response

The naming and shaming as well as the launch of an official investigation did not seem to deter the attackers from future actions. Several days after DNI Clapper publicly pointed in the direction of Russia in October 2016[58], WikiLeaks published additional emails obtained in the cyber operation against the DNC as well as Podesta[59]. After election day in November, US intelligence registered a new cyber operation of allegedly Russian origin which was targeting government employees and individuals associated with think tanks

54 http://thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war

55 https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency

56 https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/

57 https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical and https://www.eac.gov/election-officials/elections-critical-infrastructure/

58 https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html

59 http://www.politico.com/story/2016/10/john-podesta-wikileaks-hacked-emails-229304

and other institutions in the realm of national security, defense and foreign policy[60].

The president's much stronger response in December 2016 led to a verbal outburst of outrage from Russian Foreign Minister Lavrov who threatened to retaliate[61]. President Putin however decided not to escalate the situation any further. Still it is rather doubtful that Putin was truly deterred by Obama's response. It is more likely that he was just biding his time until the inauguration of then President-elect Trump who by that time was very skeptical about the attribution[62]. The publications of the NSA and CIA 'cyber arsenal' by Wikileaks[63] and Shadow Brokers[64] - which are both allegedly Russian-backed - in spring 2017 further undermine the case for the effectiveness of the US response.

Looking closely at the responses of the involved stakeholders shows a slow escalation cycle from the GCHQ tip about the DNC breach all the way to the Shadow Brokers disclosures in April 2017. There was only a small pause after Trump took office which did not see any tit-for-tat move.

Conclusion

The policy and tactical failures highlighted in this analysis start with the disconnect between government and party officials, namely FBI and the DNC. The CIA was informed about an ongoing cyber operation in autumn 2015, yet it took until April 2016 for the DNC to respond to the operation. The lack of clarity over responsibilities for cyber-defenses, investigation and remedy for the attack, and deterrent responses by the US government, plagued this incident.

In the end, it is also quite clear that the naming-and-shaming of Russia had little to no effect for deterrence of future cyber operations. Not even the holistic intelligence report could change this - with President Trump even disputing its validity (only reversing his position after repeated classified briefings). In its defense, though the IC said these details could only be included in the classified version. Even the stronger response undertaken by President Obama in January 2017 neither deterred the attacker nor did it stop the escalation cycle as the Wikileaks and Shadow Brokers disclosures suggest. As with the Parlakom case, the conclusion of the DNC episode leaves the compromised network (temporarily) in position of renewed security, but under the shadow of clear failures in the deterrence strategies.

---

60 https://www.dni.gov/files/documents/ICA_2017_01.pdf

61 https://www.nytimes.com/2016/12/30/world/europe/russia-diplomats-us-hacking.html

62 http://edition.cnn.com/2016/09/27/politics/dnc-cyberattack-400-pound-hackers/

63 https://wikileaks.org/vault7/

64 https://github.com/misterch0c/shadowbroker/

Summary and problem definition

The conclusions drawn from the two case studies suggest that there are in fact four challenges for the state when responding to cyber operations against its political IT-infrastructures:

1. disconnection/tension between political parties and different branches of government;
2. gaps in the cyber security architecture;
3. lack of confidence in (public) attribution;
4. non-deterrence of the aggressor.

Disconnection between political parties and different branches of government

Both case studies show that there is an inherent disconnection between the political entities and the government[65] when it comes to both tactical cyber security and policy responses. The political parties are rightly and necessarily independent from the government. Yet the attacks on political IT-infrastructure weaken public confidence in the integrity of elections, which is a critical concern the government must address. It has been partially addressed by the DHS response. The German case reveals that certain political parties and individual politicians within the parliament were uncomfortable with the domestic intelligence agency investigating the cyber operation. It even took several rounds of deliberation for the Bundestag's IT-committee to ask for support from the country's cyber security agency. This disconnection and its implications are highlighted even further by the fact that the parliament did not adopt the BSI's preventive cyber security mechanisms in the same fashion - which would have prevented the breach in the first place. On the contrary, this gap led to a successful foreign cyber operation against the heart of German democracy. Even after this breach (the damages for which are not yet fully inflicted), the Parlakom is still run without the full benefit of state information assurance techniques.

The US case might even be more telling. The lack of a trusting relationship between the FBI and the DNC allowed an active cyber operation to continue for months. It appears that there was neither a comprehensive communication strategy on the side of the FBI nor a trusted relationship between members of the FBI and the DNC. The loss and subsequent publication of thousands of documents as well as the breach by the second cyber operation could have been prevented by closer cooperation between the FBI and the DNC. Additionally, the DHS which is supposed to assume a leading role in cyber security, was completely absent in this case until it came time to responding politically[66]. Given the continued political debate over the role of former FBI Director Comey in the outcome of the last election, this tension appears unlikely to recede soon.

65 Especially valid for the US case is that election season increases partisanship and decreases trust. Systems need to be built in a way that they resist distrust and bridge political/ party boundaries.

66 https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

At the same time, attributing the disconnection between political entities and the government to a strategic blindness would miss the mark. All stakeholders are aware of the fact that closer cooperation would bolster IT-security. However, the separation of powers is one of the core concepts of a working democracy. Judiciary, legislature and executive branch have to be truly independent of each other. If the BSI/BfV or the NSA/DHS as parts of the executive branch would be tasked to operatively secure the political parties (legislature), they might technically also be able to monitor all communications and thereby violate the separation of powers. However, both cases show that trusted relationships and contact persons already go a long way in the event of cyber incidents. There are numerous operational changes that could be made to maintain independence and increase cyber security and incident response.

Gaps in the cyber security architecture

In the German case, members of the affected legislature were complaining about the lack of information they were receiving from the BSI and the companies during the incident handling. Likewise, representatives from the involved agencies complained that too much information was leaked to the public by the legislature which would hamper incident response. The BfV was dissatisfied by being excluded from the entire process while acting as the first stakeholder to officially attribute cyber operations.

When the DNC eventually attended the warnings from the FBI, they contracted a private information security company for incident handling and attribution. The DNC had to bring in two more companies to verify the results of CrowdStrike - especially about the claims of attribution - but the FBI was not allowed to access any of the affected systems to further their own investigation[67]. Separate from the corroborated CrowdStrike report, the DNI decided to publish its own joint report.

Having a closer look at the incident management itself, it appears that there was no strategy or plan in place on how to coordinate the response to a cyber operation of this kind. This is true for the lack of coordination among the different government branches as well as a lack of strategy within the political entity itself as to how to handle this kind of incidents. Based on what we know thus far, the technical response seemed to work out well once it was in place. The coordination and cooperation between the political parties, agencies and private sector stakeholders appeared less smooth though. In the US case the joint report was drafted without CrowdStrike's involvement, solidifying the existing gap between private and public sector involvement. In Germany, it also remains unclear how the Cyber-AZ was involved. Here again, establishing clearer plans for coordinating defense and incident response among all the stakeholders could greatly improve response times, damage control, and ultimately have a deterrent value by raising the cost and difficulty of a successful attack.

67 https://www.nytimes.com/video/us/politics/100000005151437/james-comey-live-hearing.html

Lack of confidence in (public) attribution

Even though not too many specifics are publicly known about the attackers which conducted the cyber operation against the German parliament, the head of the BfV publicly attributed the attack to Russia. It is in the nature of security and intelligence agencies that they seldom reveal information about how they come to their conclusions, but at the same time it makes it difficult to publicly justify actions that are taken based on these conclusions. Germany decided not to take any further actions apart from the weak naming and shaming and a direct diplomatic message. It is unclear if they did not have sufficient confidence in their attribution or if they were not willing to publish the evidence to justify a more far-reaching public response.

At the point where the DNC (through CrowdStrike and likely with the blessing of the White House) went public with accusations against Russia, it knew that the attribution needed to be comprehensible. They needed evidence to present it to other states but especially to their own public in order to justify subsequent actions. The special need to publicly justify the attribution arose from the naming and shaming done by the DNC in connection with the presidential election period and the alleged perpetrator's link to the presidential candidate, Donald Trump. The DNI-report which was supposed to grant this level of public attribution completely failed to do so because vital aspects were still reserved for the classified version.

In general, there are two levels of attribution. Covert operations in response to a cyber operation only need as much confidence in attribution as required by the decision-makers to feel comfortable with the decision they are making. As soon as overt activities (sanctions, naming and blaming, military) are added to the mix, it is crucial to convince the domestic and to some degree also the international public and to provide confidence about the level of attribution. In both cases, attributions offered insufficient evidence to achieve full public buy-in (or expert confirmation). The attributions were announced in ways that lacked a clear strategy for impact. And there were no public responses against Russia that appeared to rise to the level of commensurate reaction. Even though President Obama's response probably came close to that. There is an opportunity here to consider and create attribution strategies that earn greater public confidence, bridge political rivalries as well as deliver a policy result in terms of deterrence.

Non-deterrence of the aggressor

Looking at the efficiency of the responses in both cases leads to the conclusion that the attacker behind the cyber operations was not deterred at all. There are three stages when the target of a cyber operation can succeed: before the attack, during the attack and after. If there are good preventive security mechanisms in place, an attack might be rendered futile or discourage the aggressor from carrying out the cyber operation in the first place as there are possibly easier targets. During an attack, it can try to achieve some degree of damage control and deter the enemy from continuing - and possibly escalating - the ongoing operation. Afterwards deterrence is trickier because the damage is already done. However, the cyber operation can still be steered

from successful to not so successful if the response inflicts damage on the aggressor and thereby deters him from future attacks or conflict escalation. Depending on the goal of the operation, it might also become ineffective through public and media awareness even if deterrence is not successful and the attack persists - but does not get the intended attention in the media. The preventive as well as the responsive activities seem to have failed in Germany as well as in the United States. This can have a several of reasons, such as the lack of information about covert operations or the wrong target for retaliation.

Hypothesis for further research

There is an increasing demand to learn from the past to prevent future attacks from becoming successful in the books of the attacker. Deterrence might be the key to accomplish it. Deterrence theory has an ambivalent past, especially with regards to the Cold War. However, it might be prudent to revisit deterrence theory and adapt it not only to the cyber domain but specifically to cyber operations against political IT-infrastructures. President Trump tasked DHS on May 11, 2017 with finding ways to improve cyber security in the US with his Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"[68].

The problem analysis has surfaced four main challenges from the two case studies. The consequential working hypothesis is that applying deterrence theory to the problem analysis offers the potential to identify answers to these challenges[69]. Even though often limited in public and expert discourse to deterrence-by-retaliation, deterrence theory consists of four aspects: deterrence-by-denial (of benefits), deterrence-by-punishment (or retaliation), deterrence-by-norms, and deterrence-by-entanglement. Deterrence strategy always needs to consider the (military, economic, intelligence, etc.) capabilities of the deterring and respectively deterred state.

Protecting the political IT-infrastructure (a.k.a. "deterrence-by-denial")

The ultimate goal within the political setting would be to raise the level of information security to a threshold where attackers will not be able to overcome the defenses anymore. While it provides security not only against cyber operations but also cyber crime, a cost-benefit ratio is difficult to calculate when political repercussions are at stake[70]. This is a field which must be explored further. It addresses two of the primary issues raised in the case

68 https://www.dhs.gov/news/2017/05/11/president-s-executive-order-will-strengthen-cybersecurity-federal-networks-and

69 This involves better coordination and incident mitigation amongst other aspects under the strategy 'deterrence-by-denial'.

70 Traditionally "deterrence-by-retaliation" aims at raising the costs and level of difficulty for an attack so high that few try and rather look for "lower hanging fruits". When conducting cyber operations to achieve a political goal however, it stands to reason that there might not be another target that can be switched to achieve the same goal.

studies: disconnect between political entities and the government and gaps in the cyber security architecture. Concrete activities which address those challenges may include trust-building between political parties and governmental cyber security agencies as well as clear strategies and joint-responsibilities to deal with cyber operations.

However, protecting the systems is not only about preventing the attacks from being successful but also mitigating the impact of the cyber operations if they successfully breach the IT-infrastructure. It includes the segregation of networks to limit the exposure to an intruder (and keep the crown jewels secure) as well as the detection and timely removal of the attacker and the resilience to immediately recover from a cyber operation (i. e. backups).

Assessing options for show of force (a.k.a. "deterrence-by-retaliation")

This part focuses on the threat of offensive countermeasures in the event of cyber operations. For it to work, the threat must be credible and the retaliation so severe that its impact would outweigh the gains for the attacker. Attribution, zero tolerance policy, hack backs and escalation control are amongst the great challenges of getting the retaliation right and therefore need to be discussed in-depth. The punishment is not limited to the cyber domain and might even be more prudent if carried out outside of it. It mainly addresses the non-deterrence of the aggressor. If the activities which have been carried out in the past were not effective enough to deter the aggressor, this kind of deterrence helps to identify other, more appropriate responses such as economic sanctions or covert intelligence operations.

Relying on international relations (a.k.a. "deterrence-by-norms"/ "-entanglement")

This refers to the deterrence of certain activities by creating bi- or multilateral agreements[71]. Failure to comply with such agreements could result in a public naming and shaming and damage the international credibility/ respectability of the stakeholder or trigger punishments such as sanctions. It could possibly also result in a collective "deterrence-by-retaliation" (e. g. through NATO). Without proper evidence of a violation, agreements are almost impossible to enforce and therefore to be an effective tool. Nye's concept of "deterrence-by-entanglement" is a special form which relies on economic and other aspects of bi- and multilateral relationships to unfold deterring effects.

71 Examples for this are the works of the UN GGE and the OSCE, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf as well as the U.S.-China Cyber Agreement, https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html

Analyzing the pre-condition ("attribution")

The only challenge which has been identified in the problem analysis but left unaddressed so far is the lack of confidence in (public) attribution. This is of special interest as the latter two strategies ("deterrence-by-retaliation" and "-norms") require a sound understanding and superior capabilities in political, technical, legal and intelligence attribution. Those components need to be brought together to create a rating framework for the level of confidence in attribution[72]. Being able to mark the level of confidence enables the implementation of thresholds. Those thresholds serve as a basis to justify and launch retaliatory responses to cyber operations. An implementation of this rating framework might require a concerted international approach such as the establishment of an independent national/ international "watchdog" for attribution.

A framework that includes published criteria to determine attribution and thresholds for triggering types of deterrent responses have the potential to enable attribution claims that win public confidence but do not require exposure of classified evidence. Such a framework needs to factor in a degree of uncertainty for the adversary as it will otherwise face similar challenges as a zero-tolerance policy: having to act in a certain way when you do not want to. Therefore, it needs to be designed adaptive-by-design rather than in a predictable manner that can be exploited by other parties.

The case studies have demonstrated that some threat actors slowly evolve their operations from clandestine activities to a blunt, open "show of force". This warrants a strong political response, at the very least. However, credible attribution is crucial to justify those kind of high intensity responses vis-à-vis the public. The working group could therefore further study potential strategies to design and implement effective deterrence mechanisms.

72 Perfect attribution, the maximum level of confidence, could be indicated by the legal norm 'proof beyond reasonable doubt' and therefore even justify use of force as a response. This would however not be pragmatic applied to all responses as it is likely to never be reached in the cyber domain.

While we have not yet seen such a level of impact, a 'use of force' response should only be warranted under the guideline of the Tallinn Manual which stipulates that the cyber operation itself rose to the intensity level equivalent to use of force. Attribution further faces several challenges such as "false flag operations" and the public pressure for attribution which in turn supports the success of potential false flag operations.

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. TCF is an intersectoral network of experts from civil society, academia and private sector working in various areas of transatlantic cyber security and cyber defense policy. It currently consists of three working groups. This analysis has been conducted by the working group on encryption policy & lawful hacking which is composed of 35 experts. The Transatlantic Cyber Forum was made possible by the financial support of the Robert Bosch Stiftung and the William and Flora Hewlett Foundation.

Imprint

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T: +49 (0) 30 81 45 03 78 80

www.stiftung-nv.de
info@stiftung-nv.de
Twitter: @SNV_berlin

Design:
Make Studio
www.make-studio.net