CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Cyber and Information Warfare in elections in Europe

Zürich, December 2017

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Authors: Marie Baezner, Patrice Robin

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching, Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: Cyber and Information Warfare in elections in Europe, December 2017, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Cyber and Information Warfare in elections in Europe

Targets:	Integrity and legitimacy of democratic processes in France, Germany, Austria and the Netherlands; and candidates to the elections that were pro-European Union, pro-NATO and in favor of sanctions against Russia over Crimea.
Tools:	Spear phishing[1], social botnets, disinformation and propaganda.
Effects:	Raised awareness of possible cyberattacks and influence campaigns from Russia after the US presidential election; quasi absence of cyberattacks from Russia in European elections; European states being prepared for the likelihood of such activities; domestic trolls spreading disinformation campaigns, abandonment of electronic solutions in elections, multiplication of fact-checking services; cooperation between states to prevent cyberattacks from Russia, and international cooperation between trolls.
Timeframe:	From the Bundestag hack in May 2015 to the Austrian legislative election in October 2017.

After the hack of the US Democratic National Committee by Russian groups during the US presidential election, France, Germany, Austria and the Netherlands started to worry about a similar scenario occurring during their own election processes. European states and civil society actors took a series of measures to reduce the risk of cyberattacks and attempted interference through disinformation campaigns. Cyberattacks did not occur outside the presidential election in France. The major cyber-activities observed during the elections in Europe were the use and spread of disinformation in the attempt to influence the public's opinion of candidates and delegitimize democratic processes.

This report studies the cyber-activities observed during the presidential and legislative elections in France, Germany, Austria and the Netherlands. It looks at the impact of such activities on European societies, the technology employed and international relations.

There are two aims for this Hotspot Analysis. First, it seeks to develop a better understanding of the mechanisms of the use of cybertools and influence campaigns in the context of democratic processes such as elections. Second, the analysis seeks to comprehend the way states prepared for and reacted to cyberattacks and disinformation campaigns.

Description

The US presidential election of 2016 acted as a wake-up call for European countries preparing for elections in 2017. The attention was mainly focused on Russia and Russian actors as potential perpetrators during the elections. However, domestic non-state actors, such as extremist parties' sympathizers, also played a significant role in disinformation campaigns against opposing candidates. These parties did not win the elections but still managed to get good results in all of the four countries studied.

Effects

The effects of cyber-activities during the elections in Europe were mainly felt at the domestic level, in the technology sector and at the international level.

The impact of the relevant threats of foreign interference during the elections on national politics and societies were marked by a heightened awareness among European societies of such threats. States took measures to decrease the risks of meddling and emphasized the resilience of political processes in Europe in comparison to the USA. However, cyberspace was also used for influencing public opinion by domestic actors who spread disinformation campaigns against political opponents.

The technological impact of the risks of foreign interference in the elections through cyberspace manifested in the abandonment of electronic voting solutions and the rise of fact-checking tools and services.

International effects observed during the elections in European states included Western states cooperating and exchanging information on Russian threats. Similarly, extremist parties' trolls exchanged and collaborated with other sympathizers around the world, mainly sharing materials and ideas to conduct disinformation campaigns.

Policy Consequences

Policy recommendations can be derived from the experience of the threats associated with cyberattacks during the elections in Europe. The goal of such recommendations would be to reduce the risk of foreign interference through cybermeans in democratic processes. States and civil society actors can act together to expose disinformation and propaganda campaigns in order to reduce their impact. A special focus should be placed on cybersecurity measures for election and voting processes, as well as for candidates. Finally, governments could take legal measures to better frame the flow of information during election periods.

[1] Technical words are explained in a glossary in section 6 at the end of the document.

1 Introduction

The hack[2] of the US Democratic National Committee (DNC) [3] by Russian groups and the release of stolen information during the US presidential election in 2016 acted as a wake-up call for France, Germany, Austria and the Netherlands. They were holding elections in 2017 and realized that they might also become the targets of hacking and cyber influencing campaigns from foreign actors. Foreign interference in elections is not a new phenomenon, but the development and the increased use of the internet have made it easier to reach broader audiences.

This Hotspot Analysis examines how France, Germany, the Netherlands and Austria prepared to face possible foreign meddling in their election processes and to what extent the European cases were different from the US presidential election.

The study of the threat of foreign interference in the elections in these four European states is relevant because it offers an interesting comparison to the events that occurred during the US presidential election.

This analysis aims to provide a better understanding of the mechanisms of possible cyber-enabled foreign meddling in election processes. The report will be updated as new information on these four states' democratic processes is released or significant changes occur. The aim is to keep the document as current and accurate as possible. This report will also be used in a broader study comparing various Hotspot Analyses and proposing recommendations to states on ways to improve their policies with regard to cybersecurity issues.

This Hotspot Analysis is organized as follows: Section 2 defines the political and international context in which the elections and cyber-activities took place in France, Germany, Austria and the Netherlands. A chronology summarizes the main electoral events for each country as well as the main cyber-incidents.

Section 3 describes the cyber-enabled tools and techniques that were observed as having been deployed during the elections in Europe, as well as the victims and perpetrators. It shows that the cybertools used to target candidates during the elections were not technically sophisticated and that the perpetrators of disinformation campaigns included both foreign and domestic actors.

In Section 4, the report examines the effects of cyberattacks and disinformation campaigns on the elections in Europe. It shows three elements: first, democratic processes in Europe are evidently resilient; second, the political and media landscapes in Europe are more diverse and harder to influence than in the USA; third, European states were proactive in mitigating the risks of possible foreign interference in their elections; finally, trolls supporting extremist parties contributed actively to spreading disinformation about their political opponents, which might have played a role in the good results these parties achieved in the elections.

The technological effects of cyberthreats manifested as an increased mistrust in electronic solutions for elections and votes, resulting in their abandonment. Effects were also evident in the increased development of fact-checking tools and services.

The sub-section on international effects emphasizes international cooperation among states to tackle Russian interference. It also demonstrates that domestic trolls reached out to international partners to organize and exchange disinformation materials and ideas.

Finally, in Section 5, the report makes a series of policy recommendations for mitigating future foreign interference in democratic processes. It argues that states and civil society actors could work to expose disinformation and propaganda campaigns in order to reduce their impact on the population. It proposes ways for states to improve their cybersecurity during elections and legal measures to diminish the effects of the possible use of stolen documents from a previous hack.

2 Background and chronology

Awareness of how cyberattacks influence elections increased after the US presidential election of 2016. In June 2016, media outlets revealed that the US DNC's computer networks had been hacked by two Russian hacker groups. Information from the DNC was stolen and later published on the website Wikileaks at specific moments during the presidential campaign. As files were released on the internet to influence public opinion on the Democratic candidate, Hillary Clinton, concerns were also voiced with regard to potential hacks of electronic voting infrastructures. Such cyberattacks did not happen, but the events during the US presidential election and the election of the Republican candidate, Donald Trump, raised concerns in European states with elections planned for 2017.

France, Germany, Austria and the Netherlands voiced their concerns that a scenario similar to that seen in the USA might be repeated in their elections. All four states took measures to mitigate a likely cyberattack and issued public warnings that any foreign interference would be taken seriously.

[2] Technical words are explained in a glossary in section 6 at the end of the document.

[3] Abbreviations are listed in section 7 at the end of the document.

Cyberattacks only occurred in the French presidential election, but all four states experienced disinformation and propaganda campaigns from Russian media outlets and domestic trolls.

The following table summarizes the main events that occurred during the elections in the four countries. Rows with gray background refer to cyber-related incidents, while rows with light blue background list events related to elections.

Date	Event
2014	The French Front National (FN) receives a loan of €9 million from a Russian bank (Mandraud, 2017).
2015	In a report, the German Federal Intelligence Service (BND) identifies Russia as a threat to German interests in Germany and Russia.
7-8.01.2015	The Ukrainian hacker group CyberBerkut launches a Distributed Denial of Service (DDoS) attack against the German government's networks. The attack constitutes a protest against the visit of the Ukrainian Prime Minister to Germany (Stelzenmüller, 2017).
08.05.2015	The German Bundestag falls victim to a cyberattack in which approximately 16 GB of data is stolen. The attack is attributed to the Russian hacker group APT28[4], which is also believed to have ties to the Russian military intelligence (GRU) (Le Miere, 2017).
01.2016	Russian media outlets in German publish a story about a German girl being abducted and raped by three Muslims. The story is found to be false and aimed at stirring suspicion among the German population and the Muslim minority (Stelzenmüller, 2017). During the same period, German authorities discuss an appropriate way to respond to the Bundestag hack in 2015 (Beuth et al., 2017b).
24.04.2016	The first round of the presidential election in Austria sees two winning candidates, namely Norbert Hofer from the Freedom Party of Austria (FPÖ) and Alexander Van der Bellen, an independent backed by the Austrian Greens.
22.05.2016	After the second round of the presidential election in Austria, Alexander Van der Bellen wins by 50.3% (Oliphant and Cseko, 2016).
06.2016	US media reveal that the DNC's network has been hacked. It is later announced that the perpetrators are the Russian hacker groups APT29[5] and APT28.
01.07.2016	The Austrian Constitutional court overturns the results of the election of May 2016 due to irregularities. The court orders the second round of the election to be repeated before the end of 2016 (Oltermann, 2016).
26.10.2016	The French National Cybersecurity Agency (ANSSI) holds a workshop on cybersecurity for political parties and members of Parliament in anticipation of the presidential election. All political parties attend the workshop except the FN (Duguet, 2016).
10.2016	The website of Macron's party, En Marche! (EM), is targeted by a cyberattack (Chebil, 2017).
09.11.2016	Donald Trump is elected president of the USA with suspicion of Russian interference during the election.
29.11.2016	The chief of the BND warns in a press conference that Germany will most likely be targeted by foreign meddling during the election (King, 2016).
04.12.2016	Austria holds the new second round of its presidential election. This time, Van der Bellen wins by 53.3% against Norbert Hofer, who concedes defeat right after the results are out (Oliphant and Cseko, 2016).
19.12.2016	The Austrian FPÖ signs a cooperation agreement on economy, business and politics with Putin's party, United Russia (Smale, 2016).
01.01.2017	Russian media outlets publish a story about German soldiers in a NATO mission in Lithuania who allegedly raped a Lithuanian girl. The story is later proven false (Stelzenmüller, 2017).
01.02.2017	The Netherlands decides to abandon the use of vote-counting software because of concerns over potential hacking (Kroet, 2017).

[4] The hacker group is also known as Fancy Bear, Sofacy, Sednit, Strontium or Pawn Storm.

[5] The hacker group is also known as Cozy Bear, Dukes or CozyDuke.

02.2017	In a speech, the French Foreign Minister warns that France will not tolerate any foreign interference during the presidential elections. EM staff complain of being regularly targeted by attempted cyberattacks from Russia, but are unable to prove their claims. Macron is personally targeted by a series of fake allegations published mainly on Russian media outlets and relayed on social media (Reuters, 2017a; Untersinger, 2017a). The leader of the German far-right party, Alternative for Germany (AfD), holds a speech in Moscow in front of Russian members of Parliament (Branford, 2017).
01.03.2017	French President Hollande declares that all available resources will be deployed to fight cyberattacks during the presidential election (Untersinger, 2017b).
02.03.2017	German chancellor Merkel meets with Russian President Putin in Sochi to prepare for the G20 and to discuss the conflicts in Syria and Ukraine. Merkel also voices her concerns over possible meddling of Russia in the upcoming German election. Putin denies any Russian interference in foreign elections (Stelzenmüller, 2017).
06.03.2017	France decides to abandon electronic voting systems for French citizens living abroad for the legislative elections in June 2017 (Reuters Staff, 2017a).
15.03.2017	The Dutch center-right People's Party for Freedom and Democracy (VVD) wins the legislative elections and the position of Prime Minister over the far-right Party for Freedom (PVV).
24.03.2017	The French FN candidate, Le Pen, has a private meeting with Putin in the Kremlin (Mandraud, 2017).
13.04.2017	France pressures Facebook to close 30,000 accounts operated by social botnets believed to spread fake news on candidates during the presidential election (Menn, 2017; RTS Info, 2017a).
23.04.2017	Le Pen and Macron win the first round of the French presidential election.
23.04.2017	EM bans the Russian media outlets RT TV Channel and Sputnik News from covering its events (Reuters, 2017b).
25.04.2017	The cybersecurity firm Trend Micro publishes a report on the activities of the hacker group APT28. The report reveals that the hacker group registered a series of website domains with names similar to websites of Macron's campaign and two German think tanks; these could potentially be used in phishing campaigns (Untersinger, 2017a).
05.05.2017	A few hours before the mandatory pre-vote campaign media blackout, a series of documents stolen from EM computers is released on the internet under the name of MacronLeaks (Untersinger, 2017c).
07.05.2017	Macron wins the French presidential election by 66.1% (Chrisafis, 2017).
11-18.06.2017	The French legislative election takes place without any particular incident.
04.07.2017	Germany announces its concerns over potential cyberattacks from Russia during the elections in September 2017 and the possible use of documents stolen during the May 2015 Bundestag hack against candidates (RTS Info, 2017b).
24.09.2017	The Christian Democratic Union of Germany (CDU), Merkel's party, wins the German legislative election, and Merkel stays Chancellor for a fourth term. However, the election also sees the entry of the AfD into the German Parliament with 12.6% of seats (Hill, 2017).
15.10.2017	The Austrian People's Party (ÖVP) wins the majority of the votes in the Austrian legislative election (Oltermann, 2017).

3 Description

This section describes the various tools and techniques used in the elections in France, Germany, Austria and the Netherlands as well as the actors who used them and their targets. It aims to provide an overview of the actors involved in this particular context and the tools they employ.

3.1 Tools and techniques

During the various elections in Europe in 2016 and 2017, perpetrators worked with a variety of tools and techniques. Spear phishing was reported to have been used to try to get access to political party staffers' emails or political parties' networks. Social botnets were

used to attract attention, cause disruption and amplify the visibility of disinformation or propaganda messages. Unlike in the US presidential election, no political party reported that it had been hacked with malware to steal information. Even though disinformation and propaganda are not technical tools or techniques, they were extensively used during the elections in Europe and will also be treated as tools in this sub-section.

Spear phishing

Spear phishing is used to acquire victims' login credentials. The attacker sends an email that appears to come from a trusted sender in the hope that their victims would click on the link or download the attachment. If victims click on a link, they may be directed to a fake login website, where they are asked to enter their usernames and passwords. The perpetrator would then have their login information and be able to login in the victims' names. Links may also direct victims to malicious websites, where they would be encouraged to click on links that then download malware in the background and create a backdoor for the attackers. The same happens if victims download malicious email attachments.

During the various elections in Europe, several spear phishing campaigns were reported. The cybersecurity firm Trend Micro reported in April 2017 that the hacker group APT28 had registered website domain names similar to the name of the EM campaign. Trend Micro reported that such activities were also identified in Germany with names resembling those of two think tanks related to the CDU (Greenberg, 2017; Shalal, 2017). It stated that the registration of such domain names is a step towards developing spear phishing campaigns (Untersinger, 2017c). These confusing website addresses could then be used in phishing emails targeting Macron and the staff of the German think tanks. At least one of the addresses related to EM was used to obtain the login credentials of members of EM staff. It enabled hackers to get access to information that was later dumped on a website as the MacronLeaks (Associated Press, 2017). Mahjoubi, the Secretary of State in charge of Digital Affairs and then cybersecurity supervisor of Macron's campaign, declared that staff members were regularly targeted by spear phishing emails (Chrisafis, 2017).

The German Federal Office for the Protection of the Constitution (BfV) stated that it had prevented several phishing campaigns against the CDU and other political parties during the election (Dearden, 2017).

Social botnets

These botnets automatically run accounts on Twitter or Facebook. They were especially noticeable during the US presidential election, where one in five of the tweets concerning the presidential election was posted by Twitter botnets (Le Monde, 2016). The phenomenon was also observed during elections in Europe, as botnets retweeted or shared news on social media. Social botnets were mainly used as amplifiers for disinformation created by the media outlets RT (formerly Russia Today), Sputnik News and NewsFront. All three are active on Facebook and Twitter and gained popularity and visibility by using such botnets. The use of social botnets not only helped increase the visibility of stories, it also contributed to the impression that certain groups were highly popular on social media by inflating follower numbers (Nimmo, 2017).

Disinformation and propaganda

Disinformation and propaganda are not specifically technical cybertools nor are they limited to cyberspace. However, these tactics played a significant part in the elections in Europe in 2016 and 2017 and therefore need to be considered in this analysis.

The tactic is not new, but the use of the internet for activities of this nature has increased over the past few years. The tactic was regularly employed by far-right and far-left sympathizers in the elections, who used it to spread false information about their opponents on internet fora and social media in order to shape public opinion. The technique deployed by creators of fake news was to take a complex case, remove some important facts, transform the whole story and then promote it under an attention-grabbing headline. The news would then be spread around social media through social bots and amplifiers. Sometimes such fake news was republished as stories on media outlets like RT and Sputnik News. Occasionally, these stories were even shared more widely than real news on social media (Sénécat, 2017).

The construction and spread of fake news was observed in all four election processes. Trolls from far-right parties were the most visible, but far-left sympathizers also disseminated some fake news. This is partly because these political parties tend to see traditional media as corrupted and partial and regard the internet and social media as a way to disseminate an alternative narrative to the traditional media (Faye, 2017).

3.2 Targets

In the context of the elections in Europe, cyberattacks and disinformation campaigns mainly targeted the integrity and legitimacy of democratic processes, but were also aimed directly at some candidates.

Integrity and legitimacy of democratic processes

The principal targets of cyberattacks and disinformation campaigns during the European elections were the integrity and legitimacy of democratic processes. The goal was to have the wider population question such processes in order to destabilize and weaken them. Ultimately, this strategy could also be employed to weaken democratic states and show that they are no better than autocratic states (Beuth et al., 2017b; Stelzenmüller, 2017).

Candidates

The political candidates that were targeted by cyberattacks and disinformation campaigns seemed to have more or less the same profile. The victims were usually pro-European Union (EU), pro-NATO and in favor of sanctions against Russia over the annexation of Crimea.

In France, Emmanuel Macron, whose program promoted a stronger EU and defended the sanctions on Russia, was regularly targeted by disinformation campaigns and spear phishing emails and had information stolen from his network. He seemed to have become a favorite target of the disinformation campaigns spread by Russian media outlets RT and Sputnik News during the French election (Nougayrède, 2017). It went to the point that both media outlets were banned from EM events during the second round of the election (Reuters, 2017b). However, he was not the only French candidate to fall victim to disinformation, as Jean-Luc Mélenchon (candidate of La France Insoumise), Benoît Hamon (candidate of the Socialist Party) and François Fillon (candidate of The Republicans) were also targeted by far-right trolls (Sénécat, 2017).

In Germany, Angela Merkel, who defended a strong position for sanctions against Russia, was also targeted by disinformation campaigns from Russian media outlets, with some picturing her as mentally ill (Beuth et al., 2017b).

There were only few reports on targeted disinformation campaigns against specific candidates in the Austrian and Dutch elections, but both states reported that Russia conducted such campaigns (Netherlands General Intelligence and Security Service, AIVD, 2017; Simmons, 2017).

3.3 Attribution and actors

In the context of the series of elections in European states in 2016 and 2017, the concerns over foreign meddling were mainly directed at Russia. The reason for these suspicions stemmed from the events of the US presidential election and the fact that US President Obama officially accused Russia of interfering with the election. Reports published by several intelligence agencies across Europe identified Russia as a threat to the elections and public opinion. Authorities have primarily focused on Russia as a main threat, and this analysis therefore considers Russia as a main actor. However, attributing a cyberattack is not an easy task and usually based on the "*cui bono*" (to whose benefit) principle. This also means that there can be no absolute certainty in identifying the perpetrator of cyber-activities. There is always the possibility that attackers may plant false evidence to incriminate someone else, and even if Russia seemed to attract all the attention of European states, this does not mean that other actors or states were not involved.

Russia was clearly identified as a key actor in the elections in Europe, as was the hacker group APT28. Russian media outlets and trolls also played an important role in disinformation campaigns during the elections.

Russia

In recent years, Russia seems to have become the main culprit for malicious cyber-activities in Western states. Russia was primarily accused of interfering in elections and trying to influence decision-making and public opinion.

In 2013, the Chief of the General Staff of the Russian Armed Forces, Valery Gerasimov, published an essay in a military journal on the importance of non-military means in gaining superiority in conflicts. He stressed the importance of communications as a non-military means and that conflicts are won by those who best control information. The goal is to mislead the adversary by blurring the line not only between fact and fiction but also between times of war and peace. The ultimate aim is to have the adversary take decisions that would benefit and advantage Russia (Nocetti, 2015, pp. 7–8). This doctrine was used in the conflict in Ukraine and the annexation of Crimea in 2014. Cyber-activities fit perfectly into the scheme proposed by this doctrine, as they provide a cheap and stealthy means to attack an adversary's information space that can also be deployed in combination with other military operations, as was done in Ukraine (Beuth et al., 2017b).

Russia has been working on controlling its information space domestically by controlling media outlets. It also uses media outlets in foreign languages to influence public opinion in Western states. The underlying idea is not necessarily to directly influence results in elections but to cast doubts among the population regarding the trustworthiness of traditional media and state institutions (Beuth et al., 2017b).

APT28

APT28 is a Russian hacker group believed to have ties to the Russian government and the GRU, the Russian foreign military intelligence service. However, the

cybersecurity firm Trend Micro did not officially associate APT28 with the Russian government and said that such links would be difficult to prove (Associated Press, 2017). The Russian government is believed to regularly use proxy groups for performing malicious cyber-activities. By using more or less independent groups, the Kremlin is able to issue plausible denials when accused of cyberattacks.

This hacker group was first identified during the conflict between Russia and Georgia in 2008. Since then, the group has spied on defense and military targets and has been known to use spear phishing emails to get access to networks and information (Alperovitch, 2016).

Several cyberattacks and thefts of documents have been attributed to the group throughout the years. It has been accused of stealing and releasing documents from the DNC, the World Anti-Doping Agency and the German Bundestag, and to have perpetrated the cyberattack against the French TV channel TV5 Monde (Beuth et al., 2017a; Delcker, 2017). During the French presidential election in 2017, the group was observed to have registered fake website addresses to lure EM staff in spear phishing emails. APT28 was also alleged to have stolen login credentials and penetrated the EM network to steal and release documents. Reports said that metadata from stolen and dumped documents contained evidence that they had been opened at least once on a Russian computer. However, France did not officially accuse Russia or APT28 of the hack (Borger, 2017; Greenberg, 2017).

Russian media outlets

These media outlets are RT TV Channel, Sputnik News and NewsFront. They are present on the internet and present themselves as alternatives to the traditional media outlets. They are displayed in Russian as well as several other languages, including French and German. RT and Sputnik are funded by the Kremlin. NewsFront presents itself as independent, but some former employees claimed that it is funded by Russian intelligence. All three media outlets follow the Kremlin's narrative (Nimmo, 2017). They are not major media outlets in Western Europe, but they are highly visible and active on social media. They often republish each other's stories to gain visibility and credibility, as the credibility of a story increases when it is published by more than one media outlet (Beuth et al., 2017b). In their coverage of the elections in Europe, they often featured negative contributions on pro-EU and anti-Russian candidates and more positive coverage of parties sympathetic to Russia (Simmons, 2017).

Trolls

Trolls use online fora and social media to post provocative messages. The phenomenon is not new, but it gained renewed attention during recent elections in Europe and the USA. Troll profiles are often linked to far-left or far-right parties, pro-Russian, anti-Muslim and/or anti-migrant sympathizers. Trolls do not limit themselves to their own countries and often collaborate and exchange with other trolls with similar political views around the world.

In France, trolls were mostly sympathizers of the FN, who used the anonymity of online fora and social media to promote FN and controversial ideas and arguments. They tried to convince undecided voters to vote for their own preferred candidates, and they discredited other political ideas and were especially aggressive against minorities, journalists and left-wing sympathizers. The technique is not new and was already used by alt-right sympathizers in the USA during the US presidential election (Andureau, 2017), who would often start debates by posting fake news articles about political adversaries, which were frequently sourced from conspiracy websites (Motet, 2017). Moreover, their discourse often aligned with pro-Russian narratives and promoted Russian propaganda.

Similar activities were observed during the 2017 election in Germany. Two websites run by German identitarians were particularly active in promoting pro-AfD messages, neo-Nazi ideology and anti-Merkel, anti-Islam and anti-EU articles. Members of these websites were particularly active on social media to discredit the political adversaries of the AfD (Ebner, 2017).

Far-left sympathizers also participated in similar trolling activities and were also often supported by Russia. However, their online activities have been less extensively documented than those of their far-right counterparts (Meister and Puglierin, 2015).

It remains unclear if political parties were aware of such activities on the internet or if they supported them. Similarly, it is difficult to confirm if trolls were indeed party sympathizers and not trolls from a Russian troll factory who were fluent in European languages.

Table 1: Comparison of the various tools, techniques and actors that were observed in the elections in the USA, France, Germany, Austria and the Netherlands.

Events occurring during the elections/States	USA	France	Germany	Austria	Netherlands
Were documents stolen through cybermeans?	Yes	Yes	No	No	No
Did phishing occur?	Yes	Yes	Attempts	No	No
Was malware used?	Yes	Unclear	No	No	No
Was disinformation or propaganda used?	Yes	Yes	Yes	Yes	Yes
Was there the use of trolls?	Yes	Yes	Yes	Unknown	Unknown
Was there an official attribution?	Yes	No	No	No	No
Was there an investigation?	Yes	Yes	No	No	No
Was/were perpetrator(s) identified?	APT28 + APT29 (Russia)	APT28 (Russia) (unofficially accused)	No	No	No
Was there any retaliation?	Yes (diplomatic measures)	No	No	No	No

4 Effects

This section examines in detail the various effects that cyber-activities had during the elections in Europe. It looks at the way European states were impacted politically and socially, the technological changes that resulted from this context and the international effects of such cyber-activities.

4.1 Social and political effects

At the domestic political and social level, European states going through elections in 2016 and 2017 did not experience major cyberattacks like in the US presidential election. There are several reasons for this absence of significant cyber-activities. This sub-section first looks into the systemic reasons for this absence, then examines the measures taken by states to mitigate the risks of cyberattacks, the very active role of domestic trolls in disinformation and propaganda campaigns and the normalization of the use of cyberspace as a tool for influencing elections.

Systemic reasons for the absence of major cyberattacks during the elections in Europe

As soon as the US presidential election was concluded, European states organizing elections for 2017 issued statements and expressed concerns about foreign cyber-interference. European states were worried that Russia would try to influence democratic processes and opinion through hacks and disinformation, just like it was accused of having done in the USA. Nevertheless, the scenario that played out in European states was different. Anticipated cyberattacks did occur in France, but failed to deliver the same impact as in the USA. Even though similar cyberattacks were anticipated in Germany, Austria and the Netherlands, they did not eventuate.

These states took measures to mitigate the risks prior to their election dates, but there are additional reasons why foreign meddling only had limited effects. First, the absence of Russian cyberattacks can be explained by the fact that Russian meddling in the US presidential election did not have the effect that Russia would have expected. After the US presidential election, Russia found itself more isolated than before. Sanctions were not lifted by the USA but were tightened in August

2017. The USA did not reduce its commitment to NATO, and member states increased their defense spending (Thiessen, 2017). After these events, Russia might have had second thoughts about intervening in elections in Europe and might have decided not to interfere to avoid making the situation worse.

Second, in all four European states, the political and social settings were different from the USA, which probably played a role in lessening the attempts to influence public opinion. After the US presidential election, the spotlight was put on Russia and there was wider awareness of cyberattacks and disinformation from Russia, actions which it has always denied. This probably also made it riskier for Russia or Russian actors to intervene directly. They knew that as soon as any news of a cyberattack happening during a European election was published, it would be attributed to Russia. Therefore, this exposure may have deterred Russia from undertaking bolder cyber-activities (von Hammerstein et al., 2017).

Third, the media landscape in Europe is also different from the one in the USA. Traditional media are numerous and less polarized than in the USA. The press culture in Europe also has fewer tabloids newspapers and partisan news outlets than in the USA. This specific media landscape made the political context more difficult to influence, as interference would require either efforts to be targeted at very specific audiences or ways to be found to influence a whole range of news outlets (Crabtree, 2017; Hjelmgaard, 2017).

Fourth, the political landscape in Europe is just as diverse as the media landscape. In all of the four states examined, there were more than two candidates from a variety of parties running for head of state. This multitude of candidates is evidently more difficult to influence. Perpetrators are unable to focus on discrediting a single political opponent but are rather forced to attack all (Crabtree, 2017; Hjelmgaard, 2017).

Fifth, in the case of France, Macron's campaign was hacked, and documents were stolen. However, the released information was published a couple of days before the election and did not have a significant impact on the elections. A pre-existing rule that prevents any comments from the media and the candidates on the election 48 hours prior to the closing of the polling stations limited broadcasts of news of the hack, at least in traditional media[6] (Hern, 2017). This rule probably decreased the impact that the leaked information on Macron might have had on the public.

Measures taken by European states to avoid a similar scenario as in the US presidential election

The US presidential election acted as a wake-up call for these European countries and motivated them to act. Concerns over cyberattacks and disinformation campaigns were largely covered by media outlets in all four states and increased awareness among the population. Worries about cyberattacks mostly concerned Russian actors penetrating a candidate's network and releasing embarrassing information at strategic times during the campaign, as had been the case with the DNC hack. With regard to disinformation and propaganda campaigns, European politicians were concerned that voters would be manipulated by such campaigns and that they would affect votes. Often these campaigns were not aimed at directly influencing voting results but tried to discredit democratic processes and confuse public opinion by making the difference between facts and fiction more difficult to distinguish. Voters would then question the veracity and integrity of traditional media and state institutions.

The issue of propaganda and disinformation is especially difficult for democracies, as they do not control media outlets and cannot be too closely involved in declaring what should constitute the truth. Such involvement would cause states to be accused of censorship (Beuth et al., 2017b; Stelzenmüller, 2017). These issues were understood by voting European states and civil society actors, who decided to take legal and technical measures to mitigate the impacts of such potential scenarios. The latter will be discussed in Section 4.3 below.

Legal measures taken in France included state pressure on Facebook to close 30,000 accounts run by social bots that were pushing and amplifying disinformation stories (Menn, 2017). Another measure taken by France was to have the French national security agency ANSSI organize a workshop on cybersecurity to raise awareness among political parties and members of Parliament. The goal was to sensitize these groups to the fact that they are targets of interest for foreign actors. The workshop was also intended to help political parties develop good cybersecurity practices for the campaign. However, ANSSI underlined the fact that it cannot force political parties to adopt the recommended measures (Duguet, 2016).

In June 2017, Germany approved legal solutions against trolls on social media. The law contains provisions that social media companies may be fined €50 million if they do not remove posts judged to be hateful within 24 hours after receiving a relevant complaint. A similar ruling was issued by an Austrian court in 2016 (Lomas, 2017).

[6] The news was still relayed and discussed on the internet, but a majority of voters source their information from traditional media and only a minority from social media.

States were not the only ones to take action to decrease the possible impacts of foreign interference during the elections. After the US presidential election, media outlets started to create fact-checking teams in their editorial boards. These teams are in charge of fact-checking the veracity of stories or statements of candidates submitted by readers. Some also created automated fact-checking tools, which will be discussed in Section 4.3. The goal of such teams is to help readers discern between disinformation and real news.

At the level of political actors, candidates decided to act against foreign interference and disinformation. In France, Macron, having been regularly targeted with fake stories by Russian media outlets, decided to ban these media outlets from covering his party's events. However, this measure was unable to stop the release of stories targeting the EM candidate (Reuters, 2017b).

In Germany, authorities feared seeing stolen material from the 2015 Bundestag hack resurface during the election. All candidates agreed to pledge not to use social bots during the campaign and not to exploit information from the Bundestag hack if it were released by the hackers (Stelzenmüller, 2017). Also, all parties stated that they had rapid response teams for monitoring discussions on social media. Their role was to respond quickly to possible disinformation about candidates (Beuth et al., 2017b).

Domestic trolls and disinformation campaigns

Concerns about cyberattacks and meddling in elections shifted the focus of European states towards Russia. However, disinformation campaigns were also conducted by domestic actors. In France and in Germany, far-right groups conducted and contributed to disinformation campaigns against opponents of the FN and the AfD. These groups were often reusing Russian disinformation and propaganda but also developed their own stories, as was the case in France, for example, where FN sympathizers claimed that a candidate of The Republicans (center-right party), Alain Juppé, had ties to the Muslim Brotherhood (Connolly et al., 2016).

These groups have understood the usefulness of social media and the importance of giving their messages high visibility in order to influence public opinion and to give the impression that fringe groups in fact represent big crowds. Even though far-right parties did not win the elections, they managed to get good results in all states, partly due to the organizations' adoption and mastery of social media and cyberspace (Ebner, 2017). They see social media platforms as an alternative to traditional media, in which far-right parties are often negatively represented (Faye, 2017). These groups exploited general dissatisfactions and frustrations in society to polarize and exaggerate fears and discontent against migrants, Muslims, the EU, traditional media and state institutions. In the absence of this underlying sentiment, their discourses and narratives would have had less impact (Huggler and Oliphant, 2017; Vandekerkhove, 2016). They often exchanged materials with other far-right groups in Europe and in the USA (Hjelmgaard, 2017). However, it remains unclear if far-right parties participated in trolling activities. In France, the FN encouraged its members and sympathizers to be active on the internet but also tried to supervise and avoid misconduct on social media (Faye, 2017). In Germany, some members of the AfD stated that they supported online activities and even shared some links to identitarian websites known to spread disinformation (Ebner, 2017).

It was reported that far-left sympathizers were also involved in trolling activities on social media and fora, but the far-right's activities were more visible and are better documented.

Are cyberattacks during elections becoming the norm?

Other democratic states expressed concerns following the cyberattacks during the elections in the USA and France. It is likely that the issue of cyberattacks during elections and the dumping of stolen information will recur in future election and voting processes. Israeli officials have also expressed concerns that their election might be targeted by attempted cyberattacks and disinformation (Harel, 2017).

Table 2: Comparison of the measures taken by states to mitigate potential cyberattacks

Measures/States	USA	France	Germany	Austria	Netherlands
Pre-election measures to avoid the risk of cyberattacks	None	Cybersecurity workshop organized by ANSSI for candidates Ban on Russian media covering the second round of the election Deliberately planted fake documents to confuse the hackers Pressure on Facebook to close automated accounts	Pledge from all political parties not to use bots during the campaign and not to use dumps from the Bundestag hack of 2015 Creation of independent organizations to fact-check information Draft bill to force social media companies to regulate hate speech and fake news contents	Unknown	Changes to manual vote-counting procedures
Other types of measures	None	Pre-existing rule of a pre-vote campaign blackout period Abandonment of electronic voting systems for citizens abroad for the legislative election in June 2017	None	None	None

4.2 Technological effects

There has been only one reported cyberattack in the context of the elections in Europe, which did not have a significant technological impact. However, the threat of cyberattacks on elections has caused states to take technological measures to mitigate the risk of seeing their elections compromised. Media have launched automated fact-checking tools to accelerate the verification of news, social media companies have invested in fact-checking teams and tools, and a cybersecurity supervisor has demonstrated that planting fake documents in networks is able to diminish the impact of a hack.

Abandonment of electronic solutions in elections

Faced with the risk of a potential cyber-intrusion in electronic voting infrastructures during its legislative election, France decided to abandon their use for its citizens abroad[7] (Reuters Staff, 2017a). It was decided to go back to pen and paper instead, which takes more

[7] In France, electronic voting has only been available for French citizens abroad and for legislative elections since 2012 (Leloup, 2017).

time to collect and count votes but is more difficult to directly tamper with.

In a similar approach, the Netherlands decided against the use of software for aggregating results during its election and to communicate results by telephone only (Kroet, 2017). These measures show that a return to older technologies is seen as a safer approach to democratic processes. If the fear of cyberattacks becomes a recurring feature of future elections, it is likely that the development of and investment in e-voting technologies will be seriously hampered.

Multiplication of fact-checking services

Several traditional media and social media outlets have developed fact-checking procedures since the US presidential election. Some even decided to develop automated online fact-checking tools. While the majority of fact-checkers was created before the disinformation and propaganda campaigns observed during the US presidential election, these teams and tools gained in popularity and visibility after these events. Decodex[8], the automated fact-checking tool of the French newspaper Le Monde, was launched in January 2017 in preparation for the French presidential election. Its main purpose was to address growing demand by handling a larger number of requests faster. The tool operates based on a database that classifies sources as trustworthy or not. It compares a user entry with a database of media websites, blogs, Facebook pages, Twitter accounts and YouTube channels. The team managing Decodex also created a botnet on a Facebook chat to interact with users in the attempt to verify the trustworthiness of information (Les Décodeurs, 2017). Similar initiatives have also been developed in Germany[9].

Facebook announced in March 2017 that it was launching a fact-checking procedure in the USA, France, Germany and the Netherlands. This measure was taken after Facebook had been repeatedly pressured to take action against fake news and accused of being a vector for disinformation and propaganda campaigns during the US presidential election. Facebook would form partnerships with a local media outlet and a university, which would check the veracity of content on Facebook pages in their native language. When both entities agree that information is false, the information is flagged as untrustworthy but is not removed (DutchNews.nl, 2017). Facebook also invested in developing automated fact-checking features through machine learning to recognize potential disinformation articles and send them to fact-checkers for further verification (Reuters Staff, 2017b).

The development of and investment in such tools show that there is real concern about identifying trustworthy sources of information. There will probably be more technological developments in this area as machine learning and artificial intelligence evolve, pressure on social media companies grows and traditional media's determination to remain competitive against social media increases.

Deception to mitigate the effects of phishing attacks

The spear phishing attack on EM showed that unsophisticated techniques can be effective in gaining access to information. In this case, the cybersecurity manager of Macron's campaign claimed that his team had planted fake documents within the networks. These files were then found among the documents dumped on the internet labeled as the MacronLeaks. He said that no secrets were stolen and that the goal of planting such documents was to confuse hackers (Bayet, 2017). This shows that simple deception techniques can work just as well as sophisticated ones. However, the fake documents were probably not the sole element that hampered the effects of the dump on public opinion.

4.3 International effects

On an international level, the cyber-activities observed during the elections in Europe resulted in international cooperation between states to mitigate the risks of cyberattacks and cooperation between trolls to organize and spread their disinformation campaigns.

Before the election started in France and in Germany, the US intelligence community informed French and German authorities that Russia might try to interfere in the elections (MacAskill, 2017). The USA also offered its assistance in dealing with possible interference from Russia (Borger, 2017). This demonstrated that the USA was aware that Russia intended to discredit and weaken both the EU and NATO. It also confirmed that the USA was willing to prevent Russian meddling in Europe. A weaker Europe would benefit Russia and would be harmful for the USA. However, Russian interference seems to have had an opposite effect, as the EU and NATO appear to enjoy a renaissance (Stelzenmüller, 2017). The elected candidates in the European elections were mostly in favor of a strong EU and seemed to be determined to strengthen it further. NATO appears to have rediscovered its primary purpose, and its members promised to increase their defense spending (Thiessen, 2017).

International cooperation has gone beyond cooperation between states. Non-state actors such as far-right trolls have also been cooperating internationally, bringing what started as non-state

[8] For more information on Decodex: http://www.lemonde.fr/verification/

[9] Examples of fact-checking tools can be found on: https://correctiv.org/ or http://community.zeit.de/user/fact-checker

foreign influence into domestic politics. European far-right groups have cooperated and exchanged materials online among each other as well as with far-right groups in the USA and Russian groups. They have used the same online fora (4Chan, Reddit and Gab.ai) and chat applications (Discord) for exchanging techniques, strategies, photoshopped images and recruiting new sympathizers (Andureau, 2017; Ebner, 2017; Hjelmgaard, 2017; von Hammerstein et al., 2017). The stolen documents from the MacronLeaks were first relayed on social media by US far-right sympathizers before reaching France's information space (BBC Trending, 2017). This network of far-right groups shows that even though Russia had contact with far-right groups in the USA, Russia was not the sole actor trying to influence elections in Europe (von Hammerstein et al., 2017).

5 Policy Consequences

This section suggests several measures that states can take to mitigate the risks of foreign influence and cyberattacks during their election processes.

5.1 Exposing disinformation and propaganda

The main threat that European democracies faced during their elections was in fact disinformation and propaganda campaigns. This technique relies on a democratic feature that might also be considered a weakness, namely free speech. Democratic states do not control media outlets, nor are they able to censor media outlets or their citizens. As observed in this Hotspot Analysis, this is open to abuse by parties seeking to influence and discredit democratic processes .

Democracies should not try to build their own counter-propaganda discourse but should instead try to expose disinformation and propaganda articles and encourage media outlets to do the same. Yet, while denouncing false articles helps reestablish the truth, it does not address the fact that a certain number of people would have already read such false stories. Countering disinformation and propaganda is not solely the role of the state and media outlets: society as a whole needs to get involved in denouncing false articles. Media outlets already use fact-checking teams to verify information, and some also propose fact-checking tools to be used by citizens for verifying the trustworthiness of information sources, and relevant endeavors should be encouraged by the broader society.

During the elections in Europe, and after the US presidential election, it has been found that states put pressure on social media companies to better control their content. The aforementioned cases of Germany and Austria are examples of such pressures. However, this also causes the problem of having a private actor deciding whether a post should be considered hateful speech or not and should be removed or not (Benner and Hohmann, 2017). Also, simply removing posts or discussion fora does not remove the problem, it often only shifts it elsewhere. Far-right trolls are now moving from "traditional" social media, such as Facebook and Twitter, to other platforms like Gab.ai and the chat application Discord. After the discussion forum Reddit decided to close two of its sections considered to contain hateful discussions, it was found that, while the amount of hate speech diminished , it also moved to other sections of the forum to some extent (Vinogradoff, 2017).

5.2 Improving cybersecurity during elections

Cybersecurity during elections needs to become a priority for political parties and candidates. These types of actors need to realize that they may become the targets of both disinformation campaigns and cyberattacks. They often store important data on members, state and campaign issues that are of interest to foreign actors and political opponents. For these reasons, they should be encouraged to improve their cybersecurity.

France's ANSSI offered a workshop to raise this issue among political actors. Similar workshops could be repeated at each election and could also provide suggestions regarding technical solutions, such as encryption tools and messaging services, and ways to better manage files and documents to avoid easy access to sensitive information.

5.3 Taking legal measures against cyberthreats during elections

The very specific legal situation of France having a media black-out for the 48 hours prior to the closing of voting polls seems to have played an important role in hampering the impact of leaked documents from Macron's campaign. The law prevented French media outlets from commenting on the leak. Even though it did not prevent foreign media outlets and internet users from commenting, media coverage of the leak was limited.

Such measures could be adopted by other states to control the effects of possible cyberattacks during elections. However, this approach would not be efficient if stolen documents were released well before the voting day.

6 Glossary

Backdoor: Part of a software code allowing hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

Distributed Denial of Service (DDoS): Act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Domain Name Service (DNS): The address structure that translates Internet Protocol addresses into strings of letters that are easier to remember and use (Internet Corporation For Assigned Names and Numbers, 2016).

Fake News: Politically motivated, fabricated story presented as news (Teffer, 2017).

Gerasimov doctrine: Also called "non-linear warfare" or "hybrid warfare": a concept of war where all the actors are fighting each other, making alliances but also breaking them during battle. The actors only follow their own objectives and will use cyber, economic, military and psychological operations to achieve them (Miller, 2016; The Economist, 2014).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Identitarian: A term referring to a far-right political movement. Xenophobic and racist ideology that originated in France and demands the end of multiculturalism. The movement also seeks to unite nation states with the same ethnic backgrounds (Grey Ellis, 2017).

Machine learning: An artificial intelligence that can learn from the data it receives and predict outcomes without the need to be reprogrammed (Rouse, 2017).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Metadata: Information describing and explaining other data, like the date of creation of a document, the resolution of an image or the identifier of a specific device (National Information Standards Organization (U.S.), 2004).

Phishing: Technique used to trick a message recipient into disclosing confidential information like login credentials by suggesting that the message came from a legitimate organization (Ghernaouti-Hélie, 2013, p. 437).

Proxy: In computing, an intermediate server acting in place of end-users. This allows users to communicate without direct connections. This is often used for greater safety and anonymity in cyberspace (Ghernaouti-Hélie, 2013, p. 438). The term is also used in the physical world when one actor in a conflict uses third parties to fight in their place.

Social bots: Bot is a shorter term for robot. It is an automated program that runs routine tasks on social media but can also define fake social media accounts that are used to repost messages or news and/or to spam (Chu et al., 2012; Hegelich, 2016).

Spear phishing: A sophisticated malicious technique that not only imitates legitimate webpages but also selects the potential targets and adapts the malicious email to them. Often the email looks like it comes from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Troll: A person submitting provocative statements or articles to an internet discussion in order to create discord and drag more people into it (Williams, 2012).

Troll farm or factory: Place running around the clock to produce trolling messages and posts (Volchek and Sindelar, 2015).

7 Abbreviations

AfD	Alternative for Germany (German far-right party)
ANSSI	French National Cybersecurity Agency
BfV	German Federal Office for the Protection of the Constitution
BND	German Federal Intelligence Service
CDU	Christian Democratic Union of Germany (German center-right party)
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DNC	Democratic National Committee (US party)
EM	En Marche! (Macron's party)
EU	European Union
FN	Front National (French far-right party)
FPÖ	Freedom Party of Austria (Austrian far-right party)
GRU	Russia's Main Intelligence Directorate
ÖVP	Austrian People's Party (Austrian center-right party)
PVV	Party for Freedom (Dutch far-right party)
VVD	People's Party for Freedom and Democracy (Dutch center-right party)

8 Bibliography

Alperovitch, D., 2016. Bears in the Midst: Intrusion into the Democratic National Committee [WWW Document]. CrowdStrike Blog. URL https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (accessed 1.11.16).

Andureau, W., 2017. Les trolls sur Internet, nouveaux « colleurs d'affiches » du Front national [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2017/03/31/les-trolls-sur-internet-nouveaux-colleurs-d-affiches-du-front-national_5103959_4408996.html (accessed 26.9.17).

Associated Press, 2017. Hackers have targeted election campaign of Macron, says cyber firm [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/apr/25/hackers-have-targeted-election-campaign-of-macron-says-cyber-firm (accessed 27.9.17).

Bayet, A., 2017. Macronleaks : le responsable de la campagne numérique d'En marche ! accuse les "supports" du Front national [WWW Document]. Fr. Info. URL http://www.francetvinfo.fr/politique/emmanuel-macron/video-mounirmahjoubi-patron-de-lacampagne-numerique-d-emmanuel-macron-le-macronleaks-ca-pue-la-panique_2180759.html (accessed 27.9.17).

BBC Trending, 2017. Macron Leaks: the anatomy of a hack [WWW Document]. BBC News. URL http://www.bbc.com/news/blogs-trending-39845105 (accessed 13.10.17).

Benner, T., Hohmann, M., 2017. Internet Companies Cannot Be Judges of Free Speech [WWW Document]. Glob. Public Policy Inst. URL http://www.gppi.net/publications/data-technology-politics/article/internet-companies-cant-be-judges-of-free-speech/ (accessed 3.10.17).

Beuth, P., Biermann, K., Klingst, M., Stark, H., 2017a. Merkel and the Fancy Bear [WWW Document]. Zeit. URL http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia (accessed 1.10.17).

Beuth, P., Brost, M., Dausend, P., Dobbert, S., Hamann, G., 2017b. War without blood [WWW Document]. Zeit. URL http://www.zeit.de/digital/internet/2017-02/bundestag-elections-fake-news-manipulation-russia-hacker-cyberwar/komplettansicht (accessed 3.10.17).

Borger, J., 2017. US official says France warned about Russian hacking before Macron leak [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/may/09/us-russians-hacking-france-election-macron-leak (accessed 1.10.17).

Branford, B., 2017. Information warfare: Is Russia really interfering in European states? [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-39401637 (accessed 1.10.17).

Chebil, M., 2017. Quels risques de piratage pèsent sur la présidentielle française ? [WWW Document]. Fr. 24. URL http://www.france24.com/fr/20170113-quels-risques-piratage-pesent-presidentielle-francaise-anssi-cyber-attaques-russie (accessed 16.8.17).

Chrisafis, A., 2017. Mounir Mahjoubi, the "geek" who saved Macron's campaign: "We knew we were going to be attacked" [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/jun/13/mounir-mahjoubi-macron-cyber-attack-en-marche (accessed 1.10.17).

Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S., 2012. Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? IEEE Trans. Dependable Secure Comput. 9, 811–824. https://doi.org/10.1109/TDSC.2012.75

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Connolly, K., Chrisafis, A., McPherson, P., Kirchgaessner, S., Haas, B., Philips, D., Hunt, E., Safi, M., 2016. Fake news: an insidious trend that's fast becoming a global problem [WWW Document]. The Guardian. URL https://www.theguardian.com/media/2016/dec/02/fake-news-facebook-us-election-around-the-world (accessed 10.10.17).

Crabtree, J., 2017. Here's why the Dutch election is resilient to fake news [WWW Document]. CNBC. URL https://www.cnbc.com/2017/03/14/heres-why-the-dutch-election-is-resilient-to-fake-news.html (accessed 10.10.17).

Dearden, L., 2017. German spy chief warns Russia cyber attacks aiming to influence elections [WWW Document]. Independent. URL http://www.independent.co.uk/news/world/europe/germany-spy-chief-russian-cyber-attacks-russia-elections-influence-angela-merkel-putin-hans-georg-a7718006.html (accessed 1.10.17).

Delcker, J., 2017. Germany fears Russia stole information to disrupt election [WWW Document]. POLITICO. URL http://www.politico.eu/article/hacked-information-bomb-under-germanys-election/ (accessed 1.10.17).

Duguet, M., 2016. Comment le piratage informatique menace les candidats à la présidentielle [WWW Document]. FranceTV Info. URL http://www.francetvinfo.fr/monde/russie/comment-le-piratage-informatique-menace-les-candidats-a-la-presidentielle_1978011.html (accessed 1.10.17).

DutchNews.nl, 2017. Facebook to start fake news checks in the Netherlands [WWW Document]. DutchNews.nl. URL http://www.dutchnews.nl/news/archives/2017/03/facebook-to-start-fake-news-checks-in-the-netherlands/ (accessed 10.10.17).

Ebner, J., 2017. How Germany's far right took over Twitter – and tilted the election [WWW Document]. The Guardian. URL https://www.theguardian.com/commentisfree/2017/sep/26/germany-far-right-election-afd-trolls (accessed 11.10.17).

Faye, O., 2017. Le Front national, un parti en quête de contrôle sur la Toile [WWW Document]. Le Monde. URL http://www.lemonde.fr/economie/article/2017/04/01/le-front-national-un-parti-en-quete-de-controle-sur-la-toile_5104295_3234.html (accessed 26.9.17).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Greenberg, A., 2017. Don't Pin the Macron Email Hack on Russia Just Yet [WWW Document]. WIRED. URL https://www.wired.com/2017/05/dont-pin-macron-email-hack-russia-just-yet/ (accessed 27.9.17).

Grey Ellis, E., 2017. Your Handy Field Guide to the Many Factions of the Far Right, From the Proud Boys to Identity Evropa [WWW Document]. WIRED. URL https://www.wired.com/2017/05/field-guide-far-right/ (accessed 1.11.17).

Harel, A., 2017. Israeli Army Chief Warns Against Hacking of Elections, Without Mentioning Russia [WWW Document]. Haaretz. URL https://www.haaretz.com/israel-news/1.800242 (accessed 3.10.17).

Hegelich, S., 2016. Invasion of the social bots.

Hern, A., 2017. Macron hackers linked to Russian-affiliated group behind US attack [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack (accessed 27.9.17).

Hill, J., 2017. German election: A hollow victory for Angela Merkel [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-41382411 (accessed 1.10.17).

Hjelmgaard, K., 2017. There is meddling in Germany's election — not by Russia, but by U.S. right wing [WWW Document]. USA Today. URL https://www.usatoday.com/story/news/world/2017/09/20/meddling-germany-election-not-russia-but-u-s-right-wing/676142001/ (accessed 11.10.17).

Huggler, J., Oliphant, R., 2017. Russia is targeting French, Dutch and German elections with fake news, EU task force warns [WWW Document]. The Telegraph. URL http://www.telegraph.co.uk/news/2017/01/24/russia-targetting-european-elections-fake-news-eu-task-force/ (accessed 10.10.17).

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 4.11.16).

King, E., 2016. Russian hackers targeting Germany: intelligence chief [WWW Document]. POLITICO. URL http://www.politico.eu/article/german-intelligence-chief-russian-hackers-targeting-us-bruno-kahl-vladimir-putin/ (accessed 3.10.17).

Kroet, C., 2017. Dutch votes to be counted manually over hacking fears [WWW Document]. POLITICO. URL http://www.politico.eu/article/dutch-votes-to-be-counted-manually-over-hacking-fears-netherlands-election-russia-putin/ (accessed 5.10.17).

Le Miere, J., 2017. France is latest in long list of countries that have allegedly had elections hacked by Russia [WWW Document]. Newsweek. URL http://www.newsweek.com/russia-election-hacking-france-us-606314 (accessed 7.11.17).

Le Monde, 2016. Militants, trolls, bots… comment la mobilisation en ligne des pro-Trump a pesé [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2016/11/09/militants-trolls-bots-comment-la-mobilisation-en-ligne-des-pro-trump-a-pese_5028141_4408996.html (accessed 26.9.17).

Leloup, D., 2017. Législatives : les Français de l'étranger privés de vote électronique pour des raisons de sécurité [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2017/03/06/legislatives-le-gouvernement-ne-recourra-pas-au-vote-electronique-pour-les-francais-de-l-etranger-pour-des-raisons-de-securite_5090026_4408996.html (accessed 19.10.17).

Les Décodeurs, 2017. Le Décodex, un outil de vérification de l'information [WWW Document]. Le Monde. URL http://www.lemonde.fr/les-decodeurs/article/2017/01/23/le-decodex-un-premier-premier-pas-vers-la-verification-de-masse-de-l-information_5067709_4355770.html (accessed 27.9.17).

Lomas, N., 2017. Facebook must remove hate speech posts, Austrian court rules [WWW Document]. Tech Crunch. URL https://techcrunch.com/2017/05/08/facebook-must-remove-hate-speech-posts-austrian-court-rules/ (accessed 10.10.17).

MacAskill, E., 2017. US senators warn European elections are next hacking targets [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/feb/19/us-senators-warn-european-elections-next-hacking-targets-pence-trump (accessed 25.9.17).

Mandraud, I., 2017. A Moscou, Vladimir Poutine adoube Marine Le Pen [WWW Document]. Le Monde. URL http://www.lemonde.fr/election-presidentielle-2017/article/2017/03/24/marine-le-pen-recue-par-vladimir-poutine-a-moscou_5100247_4854003.html (accessed 25.9.17).

Meister, S., Puglierin, J., 2015. Perception and Exploitation: Russia's Non-Military Influence in Europe.

Menn, J., 2017. Russia used Facebook to try to spy on Macron campaign [WWW Document]. Reuters. URL http://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI (accessed 1.10.17).

Miller, C., 2016. Inside The Ukrainian "Hacktivist" Network Cyberbattling The Kremlin [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html (accessed 3.11.16).

Motet, L., 2017. Les forums de Jeuxvideo.com, fers de lance de la campagne de Marine Le Pen ? [WWW Document]. Le Monde. URL http://www.lemonde.fr/les-decodeurs/article/2017/04/02/les-forums-de-jeuxvideo-com-fers-de-lance-de-la-campagne-de-marine-le-pen_5104551_4355770.html (accessed 26.9.17).

Netherlands General Intelligence and Security Service, AIVD, 2017. Annual Report 2016. Netherlands Ministry of the Interior and Kingdom Relations.

Nimmo, B., 2017. The Kremlin's Amplifiers in Germany [WWW Document]. Medium.com. URL https://medium.com/dfrlab/the-kremlins-amplifiers-in-germany-da62a836aa83 (accessed 3.10.17).

Nocetti, J., 2015. Guerre de l'information : le web russe dans le conflit en Ukraine. Focus Strat. 62, 1–47.

Nougayrède, N., 2017. Spectre of Russian influence looms large over French election [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/apr/12/russian-influence-looms-over-french-election (accessed 26.9.17).

Oliphant, R., Cseko, B., 2016. Austria election: Far Right leader Norbert Hofer concedes defeat to Alexander Van der Bellen [WWW Document]. The Telegraph. URL http://www.telegraph.co.uk/news/2016/12/04/austria-election-norbert-hofer-cusp-becoming-europes-first-far/ (accessed 3.10.17).

Oltermann, P., 2017. Sebastian Kurz's audacious gamble to lead Austria pays off [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/oct/15/sebastian-kurz-could-31-year-olds-audacious-bid-to-lead-austria-pay-off (accessed 16.10.17).

Oltermann, P., 2016. Austrian presidential election result overturned and must be held again [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2016/jul/01/austrian-presidential-election-result-overturned-and-must-be-held-again-hofer-van-der-bellen (accessed 3.10.17).

Reuters, 2017a. French polling watchdog warns over Russian news agency's election report [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/apr/02/french-polling-watchdog-warns-over-russian-news-agency-election-report (accessed 25.9.17).

Reuters, 2017b. Emmanuel Macron's campaign team bans Russian news outlets from events [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/apr/27/russia-emmanuel-macron-banned-news-outlets-discrimination (accessed 27.9.17).

Reuters Staff, 2017a. France drops electronic voting for citizens abroad over cybersecurity fears [WWW Document]. Reuters. URL http://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233 (accessed 25.9.17).

Reuters Staff, 2017b. Facebook to step up fact-checking in fight against fake news [WWW Document]. Reuters. URL https://www.reuters.com/article/us-facebook-fakenews/facebook-to-step-up-fact-checking-in-fight-against-fake-news-idUSKBN1AJ1PF (accessed 12.10.17).

Rouse, M., 2017. machine learning [WWW Document]. TechTarget. URL http://whatis.techtarget.com/definition/machine-learning (accessed 12.10.17).

RTS Info, 2017a. Facebook cible 30'000 faux comptes en France avant la présidentielle [WWW Document]. RTS Info. URL https://www.rts.ch/info/sciences-tech/8544001-facebook-cible-30-000-faux-comptes-en-france-avant-la-presidentielle.html (accessed 3.10.17).

RTS Info, 2017b. L'Allemagne redoute une intervention russe dans ses élections de septembre [WWW Document]. RTS Info. URL http://www.rts.ch/info/monde/8752734-l-allemagne-redoute-une-intervention-russe-dans-ses-elections-de-septembre.html (accessed 1.10.17).

Sénécat, A., 2017. Comment des sites d'extrême droite fabriquent un récit « alternatif » de la présidentielle [WWW Document]. Le Monde. URL http://www.lemonde.fr/les-decodeurs/article/2017/04/03/comment-des-sites-d-extreme-droite-fabriquent-un-recit-alternatif-de-la-presidentielle_5105207_4355770.html (accessed 26.9.17).

Shalal, A., 2017. Germany confirms cyber attacks on political party think tanks. Reuters.

Simmons, A.M., 2017. Russia's meddling in other nations' elections is nothing new. Just ask the Europeans [WWW Document]. Los Angel. Times. URL http://www.latimes.com/world/europe/la-fg-russia-election-meddling-20170330-story.html (accessed 3.10.17).

Smale, A., 2016. Austria's Far Right Signs a Cooperation Pact With Putin's Party [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2016/12/19/world/europe/austrias-far-right-signs-a-cooperation-pact-with-putins-party.html (accessed 3.10.17).

Stelzenmüller, C., 2017. The impact of Russian interference on Germany's 2017 elections [WWW Document]. Brookings. URL https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/ (accessed 1.10.17).

Teffer, P., 2017. Fake news or hacking absent in Dutch election campaign [WWW Document]. EUobserver. URL https://euobserver.com/beyond-brussels/137240 (accessed 10.10.17).

The Economist, 2014. War by another name [WWW Document]. The Economist. URL http://www.economist.com/news/europe/21606290-russia-has-effect-already-invaded-eastern-ukraine-question-how-west-will (accessed 27.10.16).

Thiessen, M.A., 2017. Putin's interference in our election clearly backfired [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/opinions/putins-interference-in-our-election-clearly-backfired/2017/08/03/32fa548c-77be-11e7-9eac-d56bd5568db8_story.html?utm_term=.a01909f69b9a (accessed 13.11.17).

Untersinger, M., 2017a. La campagne d'Emmanuel Macron dans le viseur de pirates russes [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2017/04/25/la-campagne-d-emmanuel-macron-dans-le-viseur-de-pirates-russes_5117304_4408996.html (accessed 26.9.17).

Untersinger, M., 2017b. Présidentielle : les équipes des candidats sont-elles préparées aux cyberattaques ? [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2017/03/03/presidentielle-les-equipes-des-candidats-sont-elles-preparees-aux-cyberattaques_5088811_4408996.html#AbT4r4Tmutp7GDAu.99 (accessed 26.9.17).

Untersinger, M., 2017c. « MacronLeaks » : ouverture d'une enquête judiciaire en France [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2017/05/06/macronleaks-debut-d-un-long-et-fastidieux-travail-d-enquete_5123577_4408996.html?xtmc=cyber_attaque&xtcr=11 (accessed 26.9.17).

Vandekerkhove, C., 2016. La présidentielle française de 2017 peut-elle se faire pirater? [WWW Document]. BFMTV. URL http://www.bfmtv.com/politique/les-cyber-attaques-prises-au-serieux-avant-la-presidentielle-de-2017-1071345.html (accessed 17.8.17).

Vinogradoff, L., 2017. Pour venir à bout des trolls, éliminez leur espace de discussion [WWW Document]. Le Monde. URL http://www.lemonde.fr/big-browser/article/2017/09/26/pour-venir-a-bout-des-trolls-eliminez-leur-espace-de-discussion_5191856_4832693.html (accessed 27.9.17).

Volchek, D., Sindelar, D., 2015. One Professional Russian Troll Tells All [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html (accessed 22.11.16).

von Hammerstein, K., Höfner, R., Rosenbach, M., 2017. Right-Wing Activists Take Aim at German Election [WWW Document]. Spieg. Online. URL http://www.spiegel.de/international/germany/trolls-in-germany-right-wing-extremists-stir-internet-hate-a-1166778.html (accessed 11.10.17).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.