Protecting Election Integrity in the Age of Social Media: Best Practices

Report written by Līga Stafecka, associated researcher of Centre for Public Policy PROVIDUS

Riga, February 2019

Introduction

Ever since U.S. Presidential elections in 2016, the role of social networks and the threat of foreign interference has become a dominant issue in almost all discussions related to election integrity. It is especially topical for small countries, such as Latvia.

That is why two Latvia-based civil society organisations - Center for Public Policy *Providus* and Baltic Center for Media Excellence – organized an international conference „Protecting the integrity of elections: Experience of Latvia, USA, UK, Germany, Sweden and Ireland" on December 14, 2018. During the conference, representatives from several countries, representing both governmental and non-governmental sector, shared their recent experience in monitoring election integrity during 2017-2018. Their stories have been added to this report, focusing particularly on Latvia, Sweden, Germany and Ireland.

There was a consensus among all participants of the conference that elections campaigns are undergoing profound transformations. Particularly, the role of large social networks is on the rise. That is why these networks need to become more transparent, accountable and should do more to counter disinformation. In fact, according to *Special Eurobarometer 477 (fieldwork done in September 2018)*, 73% of EU citizens are concerned about online disinformation or misinformation. Citizens of some of the countries described in this report are even more concerned than an average European: 74% in Latvia, 77% in Sweden and 81% in Ireland.

The organizers of the conference hope that the case studies included in this report describing in detail the experience of 2017 federal elections in Germany, 2018 parliamentary elections in Sweden and Latvia, as well as the experience of 2018 referendum on abortion in Ireland, will be helpful to civic activists and public officials across the world to monitor their own election and referenda campaigns.

This report was made possible by support from Konrad-Adenauer-Stiftung.

Latvia (parliamentary elections of October 6, 2018)

Context

Latvia held its parliamentary elections on 6 October 2018. Both civil society organisations and state institutions monitored signs of foreign interference during the elections, and by the end of elections no such coordinated foreign-based attack was identified.

With voter turnout of 54,6%, seven political party lists managed to cross the 5% threshold. As a result of election, three new political parties entered the parliament, getting second, third and fourth best result during the elections. Political parties representing the former government were pushed down to 32 parliamentary seats out of 100.

The largest share of seats belong to the Harmony (23 seats), followed by the New Conservative Party (16 seats – new party), KPV LV (16 seats – new party), For Development/For! (13 seats – new party), National Alliance (13 seats), the Greens and Farmers Union (11 seats) and New Unity (8 seats).

According to the results of post-elections opinion survey, for many voters the voting decision was hard, and around one third of all voters made their voting decision at the last moment: during the week leading up to the Election Day. There was a very high demand for change: majority of citizens admitted that they would prefer any change to no change.

The same opinion survey uncovered the growing role of social networks during elections: around 50% of all voters had received some of election campaign information via Facebook. Nevertheless, the role of social networks should not be exaggerated: voters admitted that their decisions were primarily shaped by pre-election debates and advice received from friends and family. The competition among political parties was high, and so was the plurality of media that citizens' were using in order to orient themselves in the new political landscape.

How did state institutions of Latvia prepare for potential election interference?

Special task force

For 2018 parliamentary elections, the Government of Latvia established a special Task force – election security coordination working group. It was led by the State Chancellery – the centre of government institution in Latvia, placed under direct supervision of the Prime Minister of Latvia.

The aim of the Task force was to ensure election integrity and to protect public space from undue foreign influences. The group was headed by the prime minister's adviser on strategic communication, currently the Deputy Director of The State Chancellery Mr Kaspars Ozoliņš. It consisted of representatives of secret services (such as the

Constitution Protection Bureau or Security police), Corruption Prevention and Combating Bureau and several ministries. While the actual work of the Task force was not very visible for the broader public, the establishment of the task force got media attention.

The Task force worked in many directions: it monitored media space, established cooperation between all the public authorities having a role in securing elections and elaborated action plans relating to different election risks. The Task force also established cooperation with media.[1]

Task force monitored all main Russian media operating/accessible in Latvia, including television, radio and internet. The monitoring was conducted using confidential monitoring tools. The cooperation was also established with other institutions that conduced media monitoring for their own purposes: such cooperation was needed to double check information received by the Task force.

The Task force also established contacts with trusted media representatives abroad. If there were to be any perceived disinformation campaigns, the Task force would have informed those media.

The Task force, both on its own and also together with other state institutions, cooperated with the largest social media platforms, namely, Facebook and Google. Such cooperation was needed to agree on swift reaction procedures in case harmful or fake content would appear there. Several Facebook pages, including a fake account of a minister, were closed as a result of Task force activities.

A very significant part of the work of the Task force was to participate in common trainings/seminars with editors representing national and regional media. Those meetings were organized by Baltic Centre for Media Excellence (described in detail below).

The Task force served as the main cooperation body between all involved state institutions, held preparation meetings and followed the updates. A clear chain of commands was established in case any emergency situation arises. “We benefited from Latvia being a small country – all the responsible authorities are at an easy one-call distance. But I have to admit, our Task force was not overloaded with incoming information”, summarized Mr. K.Ozolins[2].

The main conclusion of the task force: during 2018 parliamentary elections in Latvia, there are no observations that would prove that some foreign country tried to interfere in a coordinated manner in Latvia’s elections.

For media operating in Russia, elections in Latvia were just one separate issue in the overall negative information flow about Latvia. The main coverage of Latvia’s elections disproportionally reflected just a few political parties.[3]

[1] Interview with Kaspars Ozoliņš, the Head of the Task force, 11 January 2019.

[2] Interview with Kaspars Ozoliņš, the Head of the Task force, 11 January 2019.

[3] Kaspars Ozoliņš presentation in Riga Conference“Protecting the integrity of elections Experience of Latvia, USA, UK, Germany, Sweden and Ireland” on 14 December 2018 https://www.youtube.com/watch?v=jQxjh0T0h5U

Task force observed that pro-Kremlin media channels in Latvia have comparatively small audiences that form isolated information bubbles - information published in those bubbles does not migrate to other media. Most of attempts to amplify such information through online social networks were also unsuccessful. The good news for integration of Latvian and Russian-language media spaces in Latvia: consumers of Russian-language information in Latvia increasingly prefer to visit Russian-language versions of information produced and edited in Latvia, rather than in Russia.

CERT.LV

The Information Technology Security Incident Response Institution of the Republic of Latvia provided trainings for both mass media and political parties concerning their IT security. CERT.LV provides advice not only for public institutions but also for private entities, in case they suspect that their IT systems are under cyber-attacks.

A quite sophisticated cyber-assault took place in Latvia the day before parliamentary elections. Government institutions and important internet servers were targeted, including the infrastructure of the Central Election Commission. However, the attack was unsuccessful and had no impact on the election[4]. CERT.LV did not name other institutions that were targeted and possible aggressors[5].

On the Election Day, the most popular Latvia-based social network draugiem.lv was hacked. The front page was replaced by a Russian flag and a message saying, "Fellow Latvians, this concerns you. The Russian border has no limits!" The company running draugiem.lv closed down the social network for several hours. According to the company that runs the service, no user data was compromised. Later that day CERT.LV announced that in this attack the IP addresses of Asian countries were used, but “this still does not allow to draw unequivocal conclusions about the source of the attack, because hacked equipment might have been used in the attack” and assured that the incident did not affect national security and the electoral process[6].

During recent years, public institutions in Latvia have experienced several Russian Army Intelligence Authority cyber-attacks, mainly for espionage purposes. But in context of 2018 elections, the Constitution Protection Bureau monitored the cyber space activities and concluded that they had not observed “politically motivated cyber-attacks by Russian military intelligence that would have an impact on the parliamentary elections”.[7]

Corruption Prevention and Combating Bureau (KNAB)

[4] Latvia repulsed election day cyber-attack, 18 October 2018: https://eng.lsm.lv/article/politics/election/latvia-repulsed-election-day-cyber-attack.a296457/

[5] LTV: vēlēšanu dienā bijis mēģinājums uzlauzt valsts iestādes e-pastus, 14 October 2018: https://www.lsm.lv/raksts/zinas/latvija/ltv-velesanu-diena-bijis-meginajums-uzlauzt-valsts-iestades-e-pastus.a295978/

[6] Cert.lv: Uzbrukums Draugiem.lv vēlēšanu procesu nav ietekmējis , 6 October 2018: https://www.diena.lv/raksts/latvija/politika/_cert.lv_-uzbrukums-_draugiem.lv_-velesanu-procesu-nav-ietekmejis-14206361

[7] SAB: Krievijas specdienests pēdējos gados uzbrucis Latvijas kibertelpai, 8 October 2018: https://www.lsm.lv/raksts/zinas/latvija/sab-krievijas-specdienests-pedejos-gados-uzbrucis-latvijas-kibertelpai.a295244/

KNAB oversees the legality of donations to political parties and election campaign spending limits (both by political parties and by other organisations). KNAB has a power to stop an advertising campaign if the political party or third party exceeds election spending limits during the pre-election period.

For 2018 elections, KNAB monitored advertising not just on traditional media, but also on social media. The bureau bought licenses of two monitoring tools to monitor election campaign spending on the largest internet platforms. According to Mrs Amīlija Raituma, the Head of the Party Financing Control department, the monitoring covered both paid advertisements by political parties or affiliated persons and also other political messages.[8]

Before the elections, KNAB established cooperation with biggest internet platforms – Facebook and Google. Such cooperation had not been so successful before: in context of 2017 municipal elections. Cooperation improved following several public diplomacy activities, including the President of Latvia visiting Facebook HQ in Silicon Valley as part of his visit to U.S.

Facebook provided all the requested information regarding the campaign spending on their platform. The advertising expenses declared by the political parties and disclosed by Facebook were approximately similar.

For 2018 elections, KNAB also developed a special mobile phone application that empowered citizens to report to KNAB campaigning-related problems. KNAB received a significant number of tips from citizens who were using this application.

Following elections, KNAB insists on further improvements related to social network regulation. The cooperation should not rely solely on gentlemen's agreements between state institutions and social networks. KNAB also wishes to see more guarantees that it will receive rapid replies from social networks in case of campaign law violations[9].

How did NGOs and media prepare for elections?

NGOs in Latvia have traditionally played a significant role in election campaign monitoring in Latvia. Their monitoring activities during 2002-2014 resulted in more transparent election campaigns and improved campaign regulations.

As the state institutions of Latvia became more skilled in monitoring elections, NGOs (especially, Centre for Public Policy Providus and Transparency International Latvia - Delna) started to diminish their monitoring activities. For example, they stopped monitoring attempts by political parties to circumvent campaign restrictions; they also ceased monitoring media bias, episodes of corrupt political journalism and abuse of public resources for political gains.

[8] Interview with Amīlija Raituma, representative of KNAB in charge of party financing control, 23 January 2019.

[9] Interview with Amīlija Raituma, representative of KNAB in charge of party financing control, 23 January 2019.

With the rise of social networks and threats of foreign interference, several NGOs in Latvia decided that they once again need to pay closer attention to elections in 2018. The primary organisations that coordinated their monitoring attempts were the following: Re:Baltica, Baltic Center for Media Excellence and Providus.

Firstly, they urged public authorities, especially KNAB, to prepare guidelines for political advertising on social media, and to get the necessary internet tools to monitor political ads on social networks. Secondly, these organisations worked with journalists to make them more aware of various threats to elections integrity. Thirdly, they themselves monitored activities both on traditional media and online.

Re:Baltica is a non-profit organization that produces investigative journalism in the public interest. Two month before the elections Re:Baltica conducted public monitoring of social networks. In particular, Re:Baltica monitored the content of 598 Facebook pages and 44 Facebook groups using e-tool CrowdTangle.

With crowdsourcing tool "AdCollector"[10], Re:Baltica collected political advertisements from social media, around 200-400 adds per week. In total Re:Baltica collected more than 2000 Facebook ads. People were invited to upload AdCollector extension in their computers and sort out political ads from other advertisements (for example, commercial ads, social messages, etc.). Re:Baltica provided weekly monitoring updates sharing their overall observations and screenshots of every add.

They also published short reports on each political party's activity on social media, and explored in more depth the origins of diverse online content, directly or indirectly linked to elections and candidates. By the end of election campaign, Re:Baltica came to similar conclusion as the Task force (see above): "no persuasive evidence of foreign interference was found". [11]

At the same time, Re:Baltica observed several Facebook pages during election campaign shifting from entertainment to political content, most often memes, and putting smear on mainstream political parties. Such posts had many shares and high visibility. There were also pages with extensive number of followers that suddenly switched their ownership and started to be run by politicians for electioneering purposes. According to Re:Baltica, Facebook doesn't provide sufficient information about such pages[12].

After elections, Re:Baltica criticized largest social networks for their weak (Facebook) or non-existent (Google) cooperation[13]. Inga Spriņģe, investigative journalist at

[10] The tool gathers political ads from user's Facebook News Feeds and is built by ProPublica, nonprofit investigative journalism newsroom.

[11] Inga Spriņģe: „In Russia's shadow, populists rise before the Latvian elections", 1 October 2018: https://en.rebaltica.lv/2018/10/in-russias-shadow-populists-rise-before-the-latvian-elections/?utm_source=Baltic+Center+for+Investigative+Journalism+Re%3ABaltica&utm_campaign=f63cc755a6-EMAIL_CAMPAIGN_2018_10_03_10_01&utm_medium=email&utm_term=0_37eda3a852-f63cc755a6-21086547

[12] Inga Spriņģe: *„Vai "Facebook" var nozvejot vēlētāju balsis? Var!"* 17.decembrī 2018: https://lvportals.lv/viedokli/300889-vai-facebook-var-nozvejot-veletaju-balsis-var-2018

[13] Inga Spriņģe: *„Vai "Facebook" var nozvejot vēlētāju balsis? Var!"* 17.decembrī 2018: https://lvportals.lv/viedokli/300889-vai-facebook-var-nozvejot-veletaju-balsis-var-2018

Re:Baltica, believes that international regulation for social networks is needed[14]. Jānis Sārts, director at the NATO Strategic Communications Centre of Excellence, is of a similar opinion: „It is not OK that a state has to rely on social platform to understand what is happening in its own information space. If Facebook to a limited extent was willing to cooperate, then Google was not. This should be regulated"[15].

Atlantic Council's Digital Forensic Research Lab (DFRLab) followed developments in the Latvian information space in order to detect, identify and explain unauthorized, artificial campaigns that could mislead voters. DFRLab conducts such research on everyday basis, but for election related issues it uses a special hashtag #ElectionWatch. DFRLab regularly published its observations and conclusions, [16] and it came to the same conclusions as Re:Baltica.

DFRLab paid even closer attention to Kremlin-influenced media in Latvia, where it observed strong engagement in favour of political party *Latvian Russian Union* (Latvijas Krievu savienība) and negative mentioning of political party *Harmony*.

Baltic Center for Media Excellence (BMIC) (NGO, hub for smart journalism) organized series of discussions and trainings for media and governmental institutions (both separately and together) with two aims: to raise awareness about possible threats and to coordinate activities of different institutions in various scenarios that may develop during election campaign or the Election Day.

Fortunately, the representatives from mass media and governmental institutions were ready to participate in common seminars – despite different business interests and despite lack of previous experience in organizing joint events for media editors. Everyone was well aware of the need to prepare for possible threats to election integrity[17].

BMIC organized trainings in which media editors sat at a joint table with government representatives and analysed different scenarios prepared by NATO StratCom (based on other countries' experiences in recent elections). In this way they got a clearer idea of both their own and others' responsibility. The trainings helped to discover existing loopholes and to solve them. Special attention was dedicated to regional media where seminars covered broader topics, for example, recognizing fake news and fake sources. All the aforementioned activities went beyond election period and were a significant input in strengthening information space in a longer perspective.

[14] Inga Spriņģe during the Riga Conference „Protecting the integrity of elections: what worked, what didn't?", 14 December 2018: https://www.youtube.com/watch?v=jQxjh0T0h5U&t=2953s

[15] Jānis Sārts during the Riga Conference „Protecting the integrity of elections: what worked, what didn't?", 14 December 2018: https://www.youtube.com/watch?v=jQxjh0T0h5U&t=2953s

[16] #ElectionWatch: Graphic Preference from Russian Media in Latvia. How Russian language media in Latvia visually frame political parties before elections: https://medium.com/dfrlab/electionwatch-graphic-preference-from-russian-media-in-latvia-44853a34e9c4

[17] Interview with Gunta Sloga, Director of Baltic Centre for Media Excellence, 7 January 2019.

Joint NGOs activities. NGOs engaged in numerous joint activities. BMIC, Re:Baltica and Centre for Public Policy Providus identified the most realistic threats to campaign integrity and prepared their response plans[18]. The main identified threats were the following:

- … That social media could be used for massive paid advertisement campaigns and the controlling institution (KNAB) will not be able to estimate the origin and the amount of such campaigns. This threat was monitored by Re:Baltica (as an NGO) and by KNAB (as a state institution). By the end of elections, both the society and the state institutions got a relatively clear picture about political advertising on social networks.
- … That fake news stories could be planted on social networks to influence the election results. This risk was monitored by Re:Baltica and Atlantic Council DFRLab – their work provided good insight into the sources of noteworthy fake stories appearing on internet.
- … That traditional media could be used for planting socially-divisive political content in a form of issues-based advertising, or for smear campaigns, or for discouraging voter participation. The NGOs were worried that state institution KNAB might not recognize such media content as political ads and therefore nobody would have an idea about the scale of such campaigns and their sources of funding. In order to monitor such content, Providus pre-agreed with market research company TNS Latvia that – if signs of such campaigns appear, - Providus will buy data from TNS about the scale of such campaigns and share the data with the public.
- … That fake opinion polls would be planted shortly before election date to confuse voters. PROVIDUS and BMIC commissioned (from a media monitoring agency) a clipping of media reports on opinion polls, and regularly monitored their coverage. PROVIDUS and BMIC co-organised a specific training on opinion polls for media editors as well as provided special explanatory infographics for general public[19]. The infographics were created in cooperation with *Sociologist Association of Latvia* and Organisation *School of Data.*
- … That compromising information about candidates/parties would be leaked by undisclosed sources, and the traditional media would spread such information to their own audiences. To mitigate this risk, Providus and BMIC commissioned a media clipping about political scandals, and followed their path through different media.
- … That voters will get massive amounts of election-related material from undisclosed sources in their postal mailboxes. To mitigate this risk, Providus asked to citizens, to political parties and to regional media to send samples/photos of suspicious election information that they have received via postal mail.

[18] According to written answers prepared by Iveta Kažoka, director of Providus, 21 January 2019.

[19] The infographics can be seen here: http://providus.lv/article/padomi-par-to-ka-pareizi-atainot-politisko-partiju-reitingus

Sweden (parliamentary elections on September 9, 2018)

Context

On 9 of September 2018, Sweden held general elections. Regional and municipal elections were also held on the same day.

Despite its long and strong democratic traditions, Sweden was worried about possible foreign interference in their elections. There were several good reasons for being worried.

Firstly, Sweden had already experienced its information space being threatened with destabilizing messages and cyberattacks. A number of cyberattacks were directed towards governmental institutions and political parties' websites. Before elections, public authorities had observed increases in information campaigns that were aimed at polarizing Swedish society and spreading falsehoods[20]. Swedish Military Intelligence and Security Service had stated publicly that Russia was the most frequent cyber aggressor against Sweden[21].

Secondly, after Russia had annexed Crimea in 2014, support for NATO membership in Swedish society had increased. Swedish government's cooperation with NATO intensified and "for countries that see NATO as an adversary, Sweden's shift presented a substantial threat.[22]"

Third reason was Sweden's stance on open migration policy. In relation to its population, Sweden has welcomed more refugees than any other European country– and this had taken its toll on parts of society. There had been a number of attempts to frame immigrants for crimes through fake news articles and larger disinformation campaigns. It was thought that migration-related disinformation might increase before elections. The migration issue had also been politicized by Sweden's Democrats, which is a far-right political party building its popularity on this issue.

Election turnout to Riksdag elections was the highest in more than 30 years: 87.18%. Eight political parties were elected. Social Democrats got the largest representation with 100 seats out of 349. This turned out to be the lowest level of support in several decades. The Moderate party received 70 seats, also losing its overall support, while the Swedish Democrats ranked as a third largest party with 62 seats (gained 10 seats as compared to elections in 2010).

[20] Gabriel Cederberg *„Catching Swedish Phish: How Sweden is Protecting its 2018 Elections"* https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

[21] Holmin, Maria, and Mats Knutson. *"Must-Chefen Pekar Ut Ryssland Som It-Hot."* SVT Nyheter, Sveriges Television, 12 Dec. 2016, www.svt.se/nyheter/inrikes/must-chefen-den-aktor-vi-framforallt-ser-ar-ryssland. In Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections* p.9 https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

[22] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections* p.7 https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

After elections, the Swedish Civil Contingency Agency (MSB) concluded that there was no coherent, long-term influence campaign similar to that in U.S., Germany or France during elections. Nevertheless, there were continuous attempts to influence public opinion on issues like NATO and EU, migration, stories about Sweden as a decadent society, disinformation about Swedish system, political parties, etc.[23]

MSB also commissioned a research about social networks. This research produced the same conclusions: Sweden was not affected by any direct campaigns aimed at influencing the election result. Nevertheless, the research highlighted long-term smear campaigns against Sweden presenting it as a country in decline. Even though some amplification tactics were observed, there was no evidence that those attempts had been coordinated or internationally managed. Research concluded that several media and far-right English-language chancels supported far-right groups in Sweden and presented negative, often misreported or biased reports of the country “but these were deemed to be primarily aimed at "influencing international audiences" rather than having an impact on the Swedish national election. (..) Most disinformation and misinformation relating to election fraud used real cases of mistakes or discrepancies in the election process, but amplified, sensationalised and altered the meaning of these events to the extent that they were framed as purposeful acts in a conspiracy to deny SD [Swedish Democrats] power.” [24]. Similar tactics were observed in the run-up to the recent elections in France and the U.S..

Sweden was reacting to disinformation as a part of broader national security and disaster resilience strategy, applying “whole-of-society” approach. That means that everyone was taking responsibility - central government authorities, municipalities and county councils, companies, non-governmental organisations and private individuals.

How did public authorities of Sweden prepare for potential election interference?

The main public institutions having a role in ensuring election integrity were the Election Authority, the Swedish Police Authority and the Security Service (SÄPO). Swedish Security Service (SÄPO) was mainly coordinating its cyber efforts with other Swedish government institutions, helping to strengthen its IT systems against any hacks. Election Authority was organizing elections, as well as coordinated with the local electoral commissions that are autonomous entities.

Before 2018 elections the government assigned the Swedish Civil Contingency Agency (MSB) – agency that normally is responsible for managing domestic crises like traffic accidents, chemical emergencies, natural disasters etc. – to be the lead agency and coordinate national efforts to counter disinformation and influence campaigns. It

[23] Petter Nyhlin, Civil Contingency Agency, Sweden in his presentation in Riga Conference „Ensuring integrity of elections and referenda: success stories”, 14 December 2018. https://www.youtube.com/watch?v=54Da6GIX0I4&t=11s

[24] Chloe Colliver, Peter Pomerantsev, Anne Applebaum, Jonathan Birdwell, *„Smearing Sweden International Influence Campaigns in the 2018 Swedish Election”*, ISD, Institute of Global Affairs, 2018. http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf

developed and implemented capabilities in four areas: 1) identified information influence activities by monitoring vulnerable areas in the society; 2) coordinated and cooperated between authorities and agencies conducting and protecting elections; 3) shared information among all the relevant stakeholders; 4) raised awareness about the threat with a whole-of-society approach[25].

MSB identified the main areas of possible election interference, among them were following[26]:

- Advance own political agenda (undermine trust in democracy; undermine cohesion/ destabilize countries; influence target audiences);
- Undermine trust in the election process (hacking of election management systems; physical election interference; disinformation about the reliability of election);
- Influence the will and ability of voters (disinformation about voting procedures; undermining the will to vote);
- Influence the political preference of voters (hacking political organizations; leaks of stolen information; targeting specific groups using "dark ads"; shadow financing of alternative media; trolls/ automated users manipulate social media);
- Influence/ subvert politicians (subversion of politicians and candidates and/ or political parties; subversion of government institutions).

The main remedy: awareness raising activities and coordination. Different dedicated coordination groups were set up. One of such groups was the high level National Forum, where all the aforementioned institutions took part. The National Forum carried out an extensive analysis of threats and vulnerabilities. The analysis covered Russia's attempts to influence U.S. and other European elections, methods used in these cases, and the particular vulnerabilities in Sweden. The final report was classified but it was later used to brief relevant government agencies, including local election authorities to help guide their efforts to safeguard the elections. By the Election Day, more than 7,000 civil servants at the national, regional, and local levels had received general training on influence operations and associated risks[27]. The political parties were also briefed to prepare for cyber threats and stayed in continuous contact with SÄPO until elections. All parties were provided with briefing materials from MSB and a Handbook of Personal Security from SÄPO. Several biggest parties were also strengthening their cyber security by internal cyber guidebooks. SÄPO had also distributed a handbook to 50,000 politicians at the national, local, and municipal levels that included tips and guidance about disinformation campaigns, password protection, and cyber etiquette.[28]

[25] Mikael Tofvesson, Swedish Election 2018 — A Preliminary Assessment, October 21, 2018. https://medium.com/election-interference-in-the-digital-age/swedish-election-2018-a-preliminary-assessment-bc84f5c5529a

[26] Presentation of Petter Nyhlin, Civil Contingency Agency representative in Riga Conference „Ensuring integrity of elections and referenda: success stories", 14 December 2018. ://www.youtube.com/watch?v=54Da6GIX0I4&t=11s

[27] Erik Brattbergm, Tim Maurer, *„Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks"*, May 23, 2018. Carnegie Endowment for International Peace. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[28] Erik Brattbergm, Tim Maurer, *„Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks"*, May 23, 2018. Carnegie Endowment for International Peace. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

Two more coordination groups were established, mostly for standardizing and training IT sector against possible threats.

A few months before the elections, MSB released a Handbook on influence operations for political campaign operators and local administrators, which was elaborated after extensive research conducted in cooperation with Lund University. This handbook helped to better recognize influence campaigns being carried out against them and improve their ability to respond to these threats.

According to a study from Oxford University, one in three news articles shared on Twitter with political hashtags in Sweden came from „junk news" sites but most of those „junk tweets" were home grown (eight of the top ten junk news sources)[29]. A month before election day, the presence of Twitter bots seeking to influence Swedish politics doubled and their purpose was to foment populism, promote far-right alternative news sites and support the Sweden Democrats -- Sweden's far-right, anti-immigrant party[30]. MSB established 24/7 line of communication with social-media companies, such as Facebook, Twitter and Google to report fake pages and accounts. This mechanism was mainly used to close those fake accounts that posed as government-run Facebook pages, and not all fake accounts that spread disinformation. For instance, MSB asked to close account that pretended to be a municipality account[31].

"If Crisis or War Comes" was a pamphlet produced in May 2018 by MSB. It was distributed among all Swedish households. The pamphlet suggested to critically appraise the source of information and to search for additional information, not to trust rumours and not to spread rumours[32]. „States and organisations are already using misleading information in order to try and influence our values and how we act. The aim may be to reduce our resilience and willingness to defend ourselves."

Swedish government announced nationwide curriculum reform to increase elementary and high school students' computer science skills and ability to recognize fake news. The new curriculum was officially launched in July 2018. It was directed by the Swedish Media Council. It was developed in cooperation with the Internet Foundation in Sweden (IIS), the Swedish Institute, and "Viralgranskaren," the Metro newspaper's fact-checking initiative. On its website, the Swedish Media Council also provided

[29] For every two links of professional news content shared Swedish users shared one junk news story– with 22% of all URLs shared, this was the largest proportion of junk news across all the European elections Oxford University have studied.

[30] Fact mentioned here: Ahead of election, Sweden warns its voters against foreign disinformation, 8 October 2018. https://abcnews.go.com/International/ahead-election-sweden-warns-voters-foreign-disinformation/story?id=57694373 Data from: *News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter*, September 6, 2018. Oxford University, http://comprop.oii.ox.ac.uk/research/sweden-election/

[31] Ahead of election, Sweden warns its voters against foreign disinformation, 8 October 2018. And https://abcnews.go.com/International/ahead-election-sweden-warns-voters-foreign-disinformation/story?id=57694373 and Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

[32] *If Crisis or War Comes*, Important Information For The Population of Sweden, The Swedish Civil Contingencies Agency, May 2018: https://www.msb.se/Upload/Forebyggande/Krisberedskap/Krisberedskapsveckan/Fakta%20om%20broschyren%20Om%20krisen%20eller%20Kriget%20kommer/If%20crises%20or%20war%20comes.pdf

supplemental guides for teachers to use when discussing with students online propaganda and manipulation of images[33].

In addition to these activities, high level public officials and politicians, including King of Sweden, regularly urged people to be cautious and use their critical thinking. For example, the head of Security Service urged everyone "to critically evaluate any news or rumours.[34]

One of very important aspect of Swedish case is the high level decentralization of public administration, which also implies decentralized election operations. While Swedish Election Authority is in charge of organizing national elections, there are 21 regional and 290 local election authorities that operate independently and have their own communication responsibilities. Therefore, MSB worked with all levels of election operators to raise their ability and necessary skills to recognize influence campaigns and threats. MSB had provided training on influence operations to over 10,000 public and civil servants at the national, regional, and local levels[35]. Since Sweden is relying on paper ballots and hand-counting, electronic attacks were not considered to be a high risk.

How did media prepare for potential election interference?

The traditional media of Sweden have long traditions, benefit of high public trust and are the main source of political information for Swedes. *Eurobarometer* survey indicates that Swedes are among the biggest users of written press - 57% read it daily. 88% of Swedish population use internet regularly, but distrust the information found online - only 8% of Swedes trust social networks. To compare: TV is trusted by 84% of the population and 74% trust Radio[36].

Nearly two years before the elections, at least seven biggest newspapers were subject to prolonged DDoS attacks, allegedly conducted by Russia[37]. For that reason media were well prepared and played an active role to debunk fake news and provide fact-checking to counterweight disinformation campaigns.

[33] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, p.24. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

[34] The Swedish Security Police announcement: „Risk of interference in Swedish elections 2018 January 24, 2018. https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-01-24-risk-of-interference-in-swedish-elections-2018.html

[35] Karlsson, Mattias. "Hemlig Rapport Visar Hoten Mot Svenska Valet 2018." *DN.SE*, Dagens Nyheter,17 Dec. 2017, www.dn.se/nyheter/hemlig-rapport-visar-hoten-mot-svenska-valet-2018/ In Catching Swedish Phish: How Sweden is Protecting its 2018 Elections Gabriel Cederberg https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

[36] Standard Eurobarometer 88, Report, Autum 2017 https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82873

[37] Erik Brattbergm, Tim Maurer, *„Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks"*, May 23, 2018. Carnegie Endowment for International Peace. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

Half a year before elections, five of Sweden's leading media outlets (the Swedish Public Radio, the Swedish Public Television, a digital company called KIT, and two major newspapers – Svenska Dagbladet and Dagens Nyheter) launched a fact checking collaboration called *Faktiskt*. The goal of *Faktiskt* was to fact check politicians' statements and to expose viral fake news. *Faktiskt* was supported by Swedish government to create technical platform (approx. 200 000 USD), nevertheless the platform ensured total editorial independence.

Fact checkers used different fact checking tools. For example, Dagens Nyheter used such tools as Indiana University's Botometer, BotOrNot, CrowdTangle from Facebook, and some in-house programs to monitor online information channels[38] . Each of the media involved provided fact checking on their own platforms separately. There were several additional fact checking providers.

[38] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, p.24. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

Ireland (referendum of 25 May, 2018)

Context

In 2015, Irish people voted to legalize same-sex marriage. That was an historic decision - Ireland was the first country in the world that legalized same-sex marriage via popular vote (referendum). Three years later, in 2018, people in Ireland voted on revising the Constitutional ban on abortion, in force since 1983. The Eight Amendment of the Irish Constitution banned abortion in nearly all circumstances, even to save mother's life. The referendum was held on May 25, 2018.

The referendum had a mobilizing effect on pro-life activists around the world, especially in U.S., who rallied to protect the ban. For both sides of debate the referendum seemed like an arms race where the availability of resources was of great importance. Both pro-life groups as well as pro-choice groups were supported not just in Ireland, but also had support from abroad.

The law on campaign spending did not regulate digital campaigns, that's why there were fears about the integrity of this referendum. Brexit campaign in the neighbouring country had already brought the risks of unrestricted campaigning out in the open.

Irish law prohibits donations from abroad, but this prohibition does not cover those cases when a person overseas spends directly for advertising. The worries grew when it was revealed that "Save the 8th"campaign hired the same firms that had played a part in online campaigns of Donald Trump and Brexit.

The Republic of Ireland voted in favour of overturning the abortion ban by 66.4% to 33.6%. The only constituency that voted against was Donegal, with 51.9%.

What was done to protect the integrity of this referendum?

Ireland's electoral law sets limits to the amount of campaign donations and spending. The referendum campaigns are not as clearly regulated as election campaigns. The existing regulation is outdated. For instance, the law bans foreign donations to campaigns but does not regulate expenditures on direct advertisement from abroad. That means that a foreigner cannot donate to a campaign but he or she can spend unlimited amounts on political advertising.

Transparent Referendum Initiative (TRI) decided to monitor the Irish referendum campaign on social media in order to make it more transparent and expose the online ads to the same amount of scrutiny, fact checking, source tracing as other advertising content in referendum campaigns. TRI collected the ads from social media using the scraper tool *Who targets me?* created by ProPublica. The database was crowdsourced by approximately 600 volunteers across Ireland. Altogether they collected 1500 ads related to referendum[39]. The database was open source and anyone could use it.

The monitoring indicated that organizations from abroad did in fact pay for direct ads on Facebook and Google. These ads sometimes included a clear call to action (to vote in one or the other way during referendum). Such campaigns were not transparent – there was no information about who is paying for ads and how much has been paid.

"We saw advertisements placed by groups who were registered overseas with addresses in London, in Paris, New York on their Facebook pages, paying for advertising telling people to vote one way or another. These were concrete examples that we were able to share with journalists and start to tell the story," Liz Carolan, representative of TRI, explained their findings.

TRI also found other types of untraceable information like pop-up pages or junk news pages. The TRI spotlighted such pages - after having been exposed, those pages vanished. The Initiative shared its findings, including concrete examples, with journalists. They communicated via *WhatsApp* group. This translated into good media coverage, including international media. TRI team also described their findings in a written form, hoping to raise awareness of the general population.

TRI study found that the ads were associated with approximately 224 unique Facebook pages. Only 43% of these advertisers had registered with the Standards in Public Office Commission, but the other 57% had not. The data showed that 78% of the ads were of Irish origin, with 13% coming from overseas and 9% were untraceable[40].

Social media news agency Storyful analysed the pre-referendum posts on social media. It concluded that only a third of advertisements urging a No vote (which would preserve the strict abortion law) originated from Facebook pages managed solely in Ireland. In contrast, four-fifths of posts urging repeal of the amendment were associated with pages that were managed by people in Ireland[41]. Overall, it can be said that foreign groups had strong presence during Irish referendum campaign even if one takes into account a possibility that some of the campaigners from abroad were Irish citizens living abroad.

Public pressure, social activists' persistence and coverage in traditional media were the necessary three factors to force social networks to become more transparent. TRI representative gave the following advice to civil society activists in other countries during a conference in Riga: "If you want to get Facebook to do something, get in the New York Times".

[39] The Database is available here: http://tref.ie/database/

[40] Referendum ads still appearing online despite ban – TRI, 18 May 2018, https://www.rte.ie/news/2018/0518/964431-referendum-ads/

[41] Emma Graham-Harrison, „Revealed: the overseas anti-abortion activists using Facebook to target Irish voters" 12 May 2018, https://www.theguardian.com/world/2018/may/12/ireland-abortion-campaign-foreign-influence-facebook

On 8 of May 2018, Facebook announced that "as part of Facebook efforts to help protect the integrity of elections and referendums from undue influence" Facebook will not be accepting referendum related ads from advertisers based outside of Ireland[42].

A couple of weeks before this decision, Facebook had launched the *view ads* tool. This tool enabled users to see all the ads any advertiser was running on Facebook in Ireland. Facebook also used Election Integrity Artificial Intelligence to identify fake accounts, misinformation, and foreign interference. In addition to that, Facebook launched a third-party fact-checking in Ireland through a new partnership with *The Journal.ie* that reviewed news stories, checked their facts and rated their accuracy, evaluated certain photo and video content. Some work was done to raise the voters' resilience through educational notices on how to spot false news.

Google joined a day later. On 9 May, Google announced that it was blocking all adverts on the referendum from its advertising platform and YouTube. "Following our update around election integrity efforts globally, we have decided to pause all ads related to the Irish referendum on the Eighth Amendment," the company said in a statement[43]. This decision enraged many pro-life groups whose entire strategy had relied on social media advertising which was suddenly taken away. Now it was Google that was accused of having interfered in the campaign.

Both social media giants gave very little information about these extraordinary measures. Campaigners, as well as the Transparent Referendum Initiative, called on Facebook and Google for further explanation on what they saw in their records that prompted them to act in such a manner to protect election integrity. But the companies did not make any detailed public statements to explain themselves.

[42] Facebook will not be accepting referendum related ads from advertisers based outside of Ireland. Announcement 8th of May 2018. https://www.facebook.com/notes/facebook-dublin/facebook-will-not-be-accepting-referendum-related-ads-from-advertisers-based-out/10156398786998011/

[43] Google bans abortion poll ads in Ireland. 9th of May 2018. https://www.bbc.com/news/technology-44055077

Germany (Federal parliamentary elections on September 24, 2017)

Compared to other European Union member states, social media are not very popular in Germany. Nevertheless, during the last few years Germany have experienced a large number of serious cyberattacks and disinformation campaigns organized by Russia or other actors.

"Lisa case" was one of the most prominent disinformation cases. In January 2015, a news article stated that a 13-year-old Russian-German girl Lisa had been kidnapped and raped by migrants in Germany. The story spread on Russian-language news channels and brought members of Germany's Russian-speaking minority into the streets. Later the German police proved that the story was made up and never took place. ""But the damage was already done, and the false report fed opposition to Chancellor Angela Merkel's decision to open the doors to nearly a million refugees"[44].

In May 2015, hackers infiltrated the German Parliament's computer network and 16 gigabytes of data were stolen at that time, mostly emails. The offices of at least 16 members of parliament, including Chancellor Angela Merkel's constituency office, were hit. Nearly a year later, the country's intelligence agency concluded that the attack was most likely the work of their Russian counterparts[45]. It was suspected that the stolen information would be leaked prior to 2017 elections, in a similar was as had happened during elections in France and in US.

In 2016, the group conducted an attack against the centre-left Social Democratic Party's (SPD) parliamentary group in the Bundestag as well as the state offices of Merkel's conservative Christian Democratic Union (CDU) in Saarland[46].

The Federal elections on 24 September 2017 were important – both for Germany and more internationally. Having spent 11 years in power, the chancellor Angela Merkel (CDU/CSU) was running for the fourth term. Her position was vulnerable: mostly because of unpopularity of her immigration policies. Internationally, Angela Merkel and Germany played a large role to prepare Europe's response to Russia aggression and annexation of Crimea. If Angela Merkel would have been re-elected, it would have strengthened her positions as a strong counterbalance to Russia and to rise of populism across the Western world.

[44] Melissa Eddy, *After a Cyberattack, Germany Fears Election Disruption*, December 8, 2016 https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html?module=inline

[45] Fabian Reinbold, *Germany Prepares for Possible Russian Election Meddling*, September 7, 2017 http://www.spiegel.de/international/germany/how-germany-is-preparing-for-russian-election-meddling-a-1166461.html

[46] Fabian Reinbold, *Germany Prepares for Possible Russian Election Meddling*, September 7, 2017 http://www.spiegel.de/international/germany/how-germany-is-preparing-for-russian-election-meddling-a-1166461.html

Before the Federal elections Germany experienced a rise of far-right movement. The nationalistic far-right party The Alternative for Germany (AfD) (formed in 2013) was going to enter the Parliament with a significant representation.

These are the reasons why issues of election integrity were so prominent shortly before elections. Public authorities, NGOs, political parties, media and online platforms made comprehensive preparations for elections.

The elections resulted in a fragmented parliament with six political parties. Two biggest parties decreased their representation - CDU/CSU won 33% (246 seats out of 709, loss of 65 seats from 2013), while SPD achieved its worst result since WW2 with only 20% of the vote (153 seats, loss of 40 seats from 2013). Third best result was for the far-right political party AfD, which got 12.6% (94 seats) and was elected in the Bundestag for the first time. Three other parties were Free Democrats 10.7%, Left party and Greens, each managed to get 9% of votes[47].

No significant Russian interference in the elections has been reported.

How did public authorities of Germany prepare for potential election interference?

The government of Germany rated foreign interference risk as high. That is why it took the necessary steps to prepare both for possible interference in electoral process and also for attacks targeting election campaigns directly or indirectly.

It was constantly articulated that the protection of election integrity is the highest political priority. Half a year before elections, Angela Merkel convened German Federal Security Council to discuss protection plans against Russian interference in the Federal Elections 2017. German Federal Security Council „only meets when the country faces the most serious threats"[48]. "The steps considered during the Council ranged from making potential interference as difficult and costly as possible to instigating retaliatory options if interference would occur"[49].

All the highest political authorities in Germany (President of Germany, the Head of Constitutional court and several others) called the German society to be cautious of possible disinformation campaign operations and fake news that would be aimed to influence the result of the election. As early as in spring 2017, the German government sent clear signals to Moscow that it should not dare to attempt what it did in the United

[47]Bundestag election 2017 results: https://www.bundeswahlleiter.de/en/bundestagswahlen/2017/ergebnisse/bund-99.html

[48] Erik Brattberg, Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks, Paper. Carnegie Endowment for International Peace*. May 23, 2017. Available here: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[49] Ibid.

States, France, and elsewhere[50]. Regular public announcements warned the society about risks and strengthened its resilience.

"I will simply say, such cyberattacks, or hybrid conflicts as they are known in Russian doctrine, are now part of daily life and we must learn to cope with them. We must inform people a lot on this point. (..) We cannot allow ourselves to be unsettled by this. We must simply know that this exists and learn to live with it," Angela Merkel said to media[51].

German approach was comprehensive. The Federal Returning Officer (electoral body at the federal level) was responsible for ensuring the electoral process and its integrity whereas responsibility for the election campaigns was distributed among multiple actors – local electoral agencies, political parties, politicians, and media organizations. All actors were encouraged to take responsibility to ensure the security of their own systems while the public authorities provided support if needed[52]. The Office of the Federal Returning Officer established a verified Twitter account in early 2017 for clarifying potential fake news that could disrupt the electoral process[53].

Substantial efforts were also made to strengthen cybersecurity. The Federal Office for Information Security ran penetration tests looking for vulnerabilities in computer systems and software of the Federal Election authority. The other institutions (including the Bundestag) consulted with experts about strengthening their computer security.

The public authorities also reached out to political parties in order to strengthen their cybersecurity. German domestic intelligence service shared the information on potential risks and threats to political parties. The Federal Office for Information Security (BSI) offered its services to the main political parties to help safeguard against hacking of political party computer systems as much as it was possible at that moment. The biggest political parties entered into a "gentlemen's agreement" not to use leaked information for political purposes and not to use social media bots. Trainings for political parties on basic cyber security issues were provided also by Facebook.

[50] Ibid.

[51] Melissa Eddy, *After a Cyberattack, Germany Fears Election Disruption*, December 8, 2016 https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html?module=inline

[52] Described in Erik Brattberg, Tim Maurer, Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks, Paper. Carnegie Endowment for International Peace. May 23, 2017. Available here: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[53] Fact mentioned in Erik Brattberg, Tim Maurer, Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks, Paper. Carnegie Endowment for International Peace. May 23, 2017. Available here: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

How did social networks in Germany prepare for potential election interference?

German society is still traditional in a sense that it relies on traditional media to a greater extent than in other EU member states. According to *Eurobarometer* survey, 72% Germans listen to radio daily or nearly-daily, which is the highest number in European Union. 50% Germans read written press every day or almost every day. 67% of Germans use internet every day or almost every day, but only 32% use social networks – which is the lowest number in EU[54]. The usage of social networks and trust in social networks in Germany is comparatively low. Nevertheless, the large internet platforms have been used for political party-building purposes - for instance, Alternative for Germany operates mainly via internet.

After U.S. 2016 Elections, the large internet platforms (Facebook, Google) cooperated with German Federal Office for Information Security to strengthen the integrity of the elections and protect the account of politicians and political parties from hacking.

Facebook helped to German election integrity in several ways[55]. Firstly, by ensuring authenticity. Facebook deleted tens of thousands of accounts when suspicious patterns of activity were spotted. Secondly, Facebook fought false news and reduced clickbait and spam. Third, the platform cooperated with German authorities and established a dedicated support channel for reports of election security issues¸ provided trainings for members of Parliament and candidates on online security issues. Fourth, Facebook introduced several other options for its users with the aim to encourage voters to be more informed before elections. For example, the social media offered an option for the voters to see different perspectives on the same news stories (through Related Articles function). It offered a comparison tool for political parties and the space for political parties to describe their positions on core issues.

Google and its sister company Jigsaw joined forces to defend election organizers and civic groups against cyberattacks. This defence was offered free of charge. Google expanded its Knowledge Panel to include specific information on publishers. Google also paid more attention to disinformation – which resulted in a conflict between Google and Alternative for Germany. AfD accused Google of sabotaging its campaign when Google had refused, close to Election Day, to place certain ads that promoted a controversial anti-Merkel website. The website was created by the Alternative for Germany. Google explained that the statements made in the ad and on the website were inappropriate because they could "hoax the customer".[56]

[54] Standard Eurobarometer 88, Report, Autum 2017, https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82873

[55] Update on German Elections, 27 September, 2017, https://de.newsroom.fb.com/news/2017/09/update-zu-den-wahlen/

[56] Melanie Amann and Marcel Rosenbach, *AfD Accuses Google of Sabotaging Campaign*, September 19, 2017. http://www.spiegel.de/international/germany/afd-accuses-google-of-sabotaging-campaign-a-1168757.html

How did NGOs and media prepare for potential election interference?

Media and NGOs played an important role in monitoring the election campaign and making voters more aware about possible disinformation campaigns or fake news. Media organizations set up teams of fact checkers and helped to verify the authenticity of the materials.

One of the most visible media involvements was work done by *Corrective.org*, the non-profit investigative newsroom. Several weeks before the elections *Corrective.org* was joined by *First Draft* to work together. Additional journalists were recruited from the Hamburg Media School. The collaborative pop-up group of media newsrooms was called *#WahlCheck17* and started their work four weeks leading up to the election. The team was also consulted through regular editorial meetings with the verification team at the German Press Agency.

As Claire Wardle from First Draft explained, *#WahlCheck17* monitored online conversations in real time, and alert newsrooms by publishing a daily newsletter. "These newsletters listed the most popular rumours, photoshopped images, manipulated videos, and misleading articles and data visualizations circulating online, offering contextual information about the sources, relevant data and the results of forensic social verification techniques" [57].

#WahlCheck17 used ad combination of different tools such as Crowdtangle, Facebook Signal, Google Trends, NewsWhip Spike, Trendolizer, Trendsmap (to keep track specifically of Twitter trends by location), Botswatch (to map bot networks) and TweetDeck. The group was collecting large number of posts from Twitter, Facebook, Reddit and 4Chan to analyse conversations online from relevant pages, groups and accounts. To increase the visibility of fact-checked information, the team used the Fact-Check Tag for Google Search and Google News[58].

#WahlCheck17 concluded that "Misinformation didn't change the outcome of the Bundestag election, but it still made headlines. The volume and maliciousness of disinformation never reached the level that it did in the lead-up to the elections in France. But some trends did emerge. Still, many pieces of disinformation focus on the topic of refugees and Muslim immigrants, and individual politicians were often subjects and victims of false information. Mis- and dis-information circulated within narrow target groups, such as anti-Muslim Facebook groups, and regionally based communities"[59].

[57] Claire Wardle, *#WahlCheck17: Monitoring the German election*, September 1, 2017. https://firstdraftnews.org/wahlcheck17-correctiv/

[58] Ibid.

[59] Ingrid Brodnig, *7 types of misinformation in the German election*, November 7, 2017. https://firstdraftnews.org/7-types-german-election/

There were several other activists that also monitored the informative space and analysed the amplification of the content. For example, *Artikel38 Dashboard*, that monitors Russian influence operations on Twitter that targets German-language audiences[60].

A September 2017 study by Oxford University found that although the far right in Germany did employ automated Twitter profiles known as “bots”, traffic from those accounts was relatively low and ineffective. The study concluded: „Social media users in Germany have shared many links to political news and information, but links to professional news have outnumbered those to junk news by a ratio of four to one”[61].

[60] The methodology is described here: https://securingdemocracy.gmfus.org/methodology-of-the-artikel-38-dashboard/

[61] *Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?* Oxford University, September 19, 2017 http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/09/ComProp_GermanElections_Sep2017v5.pdf