CHAPTER 7

Institutional Responses of European Countries

Jan Hanzelka and Miroslava Pavlíková

7.1 Introduction

After the Ukrainian conflict began in 2014, disinformation campaigns were identified in various European countries. Occurrences like the Brexit campaign '#leave' influence operations during parliamentary elections in Europe (in Germany or France, for example) or domestic active measures scandals, such as Austria's Freedom Party of Austria (FPÖ) stressed the need to counteract such tactics and protect targets—nation states as well as supranational structures. The dynamics of influence operations and forms of disinformation dissemination are very fast, flexible, and even harder to maintain.

In reaction to the latest disruptive propaganda campaigns in Europe, the institutions of some countries have focused on countermeasures. Some include the establishment of special governmental bodies, the installation of special task force groups, new laws, and active cooperation

J. Hanzelka · M. Pavlíková (✉)
Department of Political Science, Faculty of Social Studies, Masaryk University, Brno, Czechia

M. Gregor and P. Mlejnková (eds.), *Challenging Online Propaganda and Disinformation in the 21st Century*, Political Campaigning and Communication,
https://doi.org/10.1007/978-3-030-58624-9_7

between governments, political parties, media, non-governmental organisations, and academia. However, particular counter steps, the willingness of authorities, and the adequacy of measures differ. This chapter analyses how European countries deal with malicious online disinformation and propaganda. We will assess the European state authorities' and institutions' countermeasures against information warfare, especially the good examples and specific approaches of particular countries. The text focuses on lessons from election interference and the preparedness of particular countries, taking into consideration long-term measures as well. According to the mentioned approaches, we have formulated a categorical framework for the analysis of institutional countermeasures, which we then use to analyse the cases of several European countries.

Actors who aim to defend themselves against propaganda and disinformation campaigns need to study the newest cases, technologies, and tactics to counter these hostile activities effectively. Although we can perceive coordination efforts on the international level, there are still many differences between European states in their approaches to countermeasures. There are good examples of preparation, active responses, as well as coordination and the sharing of good practices among states. On the other hand, some actors still have a lot to learn. In this chapter, we will focus on three examples from across Europe: The case of Denmark demonstrates a country which has a leading position in countermeasure formulation; in central Europe, Czech Republic is an example of a country which is 'half-way'; and the south-eastern European country of Bulgaria reveals a country with barely noticeable measures. All three countries are members of the European Union and NATO. However, all three have different approaches to challenging propaganda and disinformation, and they thus make evident how different political attitudes, different histories, and different starting positions can affect the approach towards countermeasures.

7.2 Framework for Analysis: Institutional Countermeasures Against Influence Operations

In the following section, a framework with types of institutional responses for the complex analysis of case studies is proposed. In this chapter, influence operations instead of disinformation and propaganda are often mentioned, even though this concept is more complex and also covers other activities (see Chapter 1). The reason is European states' usage of

influence operations in its proclamations and documents. Countermeasures against disinformation and propaganda are often part of the bigger package covered under the influence operations' umbrella.

The particular categories are derived from the most viable countermeasure examples found in different European countries and existing frameworks, which have been evaluated as relevant and actual. The framework proposal by Brattberg and Maurer (2018) of the Carnegie Endowment for International Peace serves as inspiration in its consideration of good examples from chosen European countries (Germany, Sweden, France, and Netherlands). It focuses on resilience and legal measures, public statements, and the education of voters as it concerns disinformation campaigns. They also suggest training and educating political parties, conducting government-media dialogue, engaging media companies to mitigate threats, and, finally, sharing lessons learned as well as best practices to support international cooperation. Moreover, the authors suggest clearly warning citizens about possible interference, promoting citizen fact-checking and investigative journalism, and urging political parties to assert that they will not use social media bots. This might generally cover avoidance of negative campaigns and usage of disinformation, as well as placing stress on transparency (see Flamini and Tardáguila 2019). The analysis is secondly inspired by the categorisation of the Ministry of Foreign Affairs of Denmark, which presented 11 initiatives to counter hostile influence operations. Besides the abovementioned responses, Denmark suggests the establishment of an intergovernmental task force to strengthen the monitoring of disinformation, train communication officers, and reinforce intelligence services activities (Ministry of Foreign Affairs of Denmark 2018).

The following section will introduce particular categories and their measures. Furthermore, examples of real countermeasure usage will be explained with a focus on European countries. These examples have been chosen based on the availability of information and the possible effectivity of the countermeasures. The aim is to focus on good or even best practices. However, it is obvious, that some countermeasures are unique and evaluation on effectivity needs historical distance. In accordance with an index from the European Policy Initiative of the Open Society Institute (2018, In: Mackintosh and Kiernan 2019) measuring the post-truth phenomenon in countries, the Scandinavian countries, Estonia, and the Netherlands rank first. If possible and available, good examples from these countries are described in more depth. Besides European countries, we

also focus on the supranational level. Countermeasures from the European Union and NATO will also be assessed, including the actions of particular European countries in regard to these supranational entities. We consider this one of the categories for analysis, and it is listed in Table 7.1.

7.2.1 Actions with the Public

The institution of *clear warning* resonates especially with the secret services or other governmental bodies in terms of its impact on security. Secret services might occasionally present warnings about serious security issues or present actual threats in their annual public reports. Warning by secret services might have greater value for the public than the proclamations of other authorities. In the Netherlands, for example, the 2018 annual public report of the General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst in Dutch) mentioned covert

Table 7.1 Categorisation of institutional countermeasures against influence operations

Category	*Activities*
Actions with the public	Clear warnings Public statements Voter education Education of parties
State measures	Establishment of special ministerial bodies or other state institutions Employee education
Legal measures	Implementation of legal measures Cooperation with business
Actions with the media	Train communication officers Strengthen disinformation monitoring Support investigative journalism
Actions with political parties	Urge parties into political culture compliance Organise training for political parties and campaigners
Direct countermeasures	Information operations against hostile actors Diplomatic pressure
Actions with supranational entities	Cooperation Join task forces Join discussions Accept recommendations

Source Authors

influence and manipulation of the public perception by Russia and China (General Intelligence and Security Service 2018). It also informed about surveillance by the Russian hacking group Cozy Bear, after which they publicly attributed an attack to Russia (Brattberg and Maurer 2018). In a public report from March 2019, the Estonian Foreign Intelligence Service (Valisluuveramet) warned about the Russian threat before the European parliamentary election, revealing that France, Germany, and Italy were the main targets (Estonian Foreign Intelligence Service 2019; EU Observer 2019). The report considers cyber threats by Russian secret services especially, in addition to mention of troll activities, to be an integral part. A recent Estonian report also stresses that 'China is more and more active in influence operations and propaganda'. Islamic State propaganda in Europe is also highlighted. In May 2019, the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz) in Germany, warned against the Austrian government (saying it could not be trusted) because of its ties to Russia and a possible information flow between them (Stone 2019). The whole warning derives from the activities of the then governing party FPÖ, the Russians, and negotiations about the production of favourable media coverage.

Naturally, a lot of clear warnings or public attributions were made by governments, politicians, and other high state authorities. French President Emmanuel Macron, the British foreign secretary at the time, Boris Johnson, as well as German chancellor Angela Merkel warned against Russian interference into election processes (Brattberg and Maurer 2018). This might be connected to *public statements* and *voter education*, which is often utilised by governments or authorities. An interesting example can be found in the French government's clear labelling of Sputnik and RT as pro-Kremlin outlets, and their subsequent exclusion from press conferences in Élysée Palace as well as regular refusal in covering official events (EUvsDisinfo 2019). The Swedish Civil Contingencies Agency, under the Ministry of Defence, launched an awareness campaign for *public education* about propaganda (Robinson et al. 2019). In a 20-page-long document called *If Crisis or War Comes*, a chapter about false information has its place with easily written advice and interactive questions (Swedish Civil Contingencies Agency 2018). The government also planned to teach children in primary schools how to recognise fake news (Roden 2017). A similar governmental approach appeared in Finland as well (Charlton 2019). CNN labelled Finland a country which is winning the war on fake news (Mackintosh and Kiernan 2019). The government's anti-fake news

programme is based on cross-departmental engagement, learning best practices from around the world, and a bottom-up approach starting with country's education system[1] (KennyBirch 2019). Public governmental campaigns in the United Kingdom have intensified after the Skripal case. Shortly after the attack, the UK government established communication teams which informed the public about Russian manipulative tactics. Currently, the British government is starting a public campaign focused on empowering citizens in disinformation recognition and awareness of its malicious effects. The campaign started with the issue of measles and vaccination against it.

7.2.2 State Measures

State measures is mostly meant as the formation of special governmental or state bodies, strengthening the role of institutions in the influence operations fight, and other intragovernmental provisions. In some countries, *special task forces* or other ministerial bodies have been established to counter-influence operations. In 2017, as a reaction to Russian activities, the Danish government established an inter-ministerial task force for countering these campaigns. This special body coordinates efforts across government as well as Danish national intelligence and security services (EUvsDisinfo 2018). In Sweden, for example, a psychological defence authority (psykologiskt försvar) has been launched. This authority focuses on countering disinformation and boosting the population's resistance to influence operations. In the Netherlands, the National Coordinator for Security and Counterterrorism received in 2019 responsibilities related to the detection of influence operations run by foreign state powers. In Czech Republic, the Ministry of the Interior established the Centre Against Terrorism and Hybrid Threats for expert and analytical activities, including disinformation campaigns (Ministry of the Interior of the Czech Republic 2017). Its activities remain mostly classified. In Ukraine, meanwhile, a whole ministry focusing on information policy was founded. The ministry was established to fight against information attacks (Interfax-Ukraine 2014). In 2019, it presented a white book on information operations against Ukraine (*Bila kniga specialnih informacijnih operacij proti Ukraïni*, see Ministry of Information Policy of Ukraine

[1] For example, the project for schools called 'Facts, please!'.

2018) considering Russia's influence operations in the country between 2014 and 2018 (Ukrainian Independent Information Agency of News 2019).

As regards *state employee education*, Finland launched a programme on countering propaganda for government officials. The programme emphasises the importance of creating a new narrative which highlights Finnish values and a 'Finnish story' (KennyBirch 2019). In Sweden, the Civil Contingencies Agency produced a manual countering information operations which might target public service workers (Klingová and Milo 2018). *Countering Information Influence Activities: A Handbook for Communicators* (Swedish Civil Contingencies Agency 2019) provides techniques and advice on how to counter information influence operations, including preparing organisations for a quick and effective response.

7.2.3 Legal Measures

Focusing on legal measures would take an entire chapter or even book (see Chapters 4 and 6 for European level of legal measures), thus we will cover only special laws reacting to disinformation. In Italy, for example, citizens can use a special online service where it is possible to report fake news to the police (Robinson et al. 2019). After abandonment of this measure, a bill proposing sentences for spreading fake news was tabled in 2017. In 2017, Germany passed a law called NetzDG which is meant to combat fake news and hate speech on the Internet. Under this law, social media platforms have 24 hours after receiving a report to remove a post which violates German law. It furthermore forces networks to reveal the identities of those behind posts. The law has become a subject of discussion about freedom of speech violations (Bleiker and Brady 2017).

In 2018, the French parliament passed a law related to election campaigns, according to which the electoral jurisdiction has a responsibility to decide on the withdrawal of manipulative materials from the Internet. However, there must be evidence that such material was intentionally spread on a wide scale with the intention of interfering and disrupting the elections (Rozgonyi 2018).

Nevertheless, these legal measures have a few weaknesses. First of all, they mix together terrorist content, hate speech, and acts that are part of influence operations. However, influence operations may demand different counter approaches than terrorist propaganda. Secondly, the

legal measures focus on content and do not deal with the tools and techniques of influencing, for example, the use of fake accounts, bots, and algorithms.

Currently, we can see a trend in the efforts of European governments to engage the cooperation of Facebook and Google in the case of negative social issues.[2] General efforts, such as systematic work towards 'stopping of misinformation and false news' can be seen. In Facebook's 'Community Standards' there is a paragraph which reads, 'There is also a fine line between false news and satire or opinion. For these reasons, we do not remove false news from Facebook, but instead significantly reduce its distribution by showing it lower in the News Feed'. The article is part of a broader Facebook strategy to handle fake news (Facebook 2019). This solution is dependent on the problematic identification of fake news without deep research and fact-checking. They are trying to avoid accusations of political persecution from certain opinion groups, which would otherwise be faced with the deletion of content. In certain countries (Facebook 2020), Facebook has third-party fact-checking partners. There, partners are trained to assess the truth of a post and, in the case of fake news, use predefined tools to limit the available contributions or prohibit monetisation (Facebook 2020). Google has a similar initiative, which is described in the white paper *How Google Fights Disinformation* (Google 2019). The Google initiative is based on ranking and labelling content, and the results are reflected in the search algorithm. Less credible news is less relevant in a search. Google declares that they 'welcome a constructive dialogue with governments, civil society, academia, and newsrooms' (Google 2019).

7.2.4 Actions with the Media

Cooperation with media might play a key role in controlling the disinformation flow as well as promoting media literacy. Belgium provides an example of an active approach from government to media. The Flemish Ministry of Education and Training sponsors Média Animation ASBL, a media education resource which focuses on media literacy in schools as well as for politicians and other decision-makers (Kremlin Watch 2020;

[2] An example is the problem of hate speech and current German legislation, which is trying to delegate responsibility for this issue to social media providers (Hanzelka and Kasl 2018).

Media Animation ASBL 2020). The Swedish government also expressed the will to cooperation with media when the government, together with the Swedish national television broadcaster, invested in a digital platform providing automatic fact-checking and news in a way which crosses the borders of filter bubbles. In Latvia, we can find an example supporting investigative journalism since 2017. The new programme was launched under the auspices of the Ministry of Culture, and it has financially supported about 20 projects (Robinson et al. 2019). Another interesting example of an approach to media can be found in Estonia. Its politicians and administration officers claim they never give interviews to Russian state-controlled media (Sternstein 2017). Some countries must also deal with its Russian minorities and the need for Russian-language media; this is mostly relevant in the Baltic countries. Estonia started its own Russian-language channel in 2015. This repression of Russian-language sources with connections to the Russian government is also a strategy some countries deploy to protect minorities. In Lithuania, for example, the government pulled RTR-Planeta, run by the Russian government, off the air (PressTV 2017; Sternstein 2017).

7.2.5 Actions with Political Parties

There are many discussions over voter education about disinformation, but little is said about the education of political parties. Moreover, as for example the Brexit referendum has shown,[3] political parties might have a strong role in the spread of disinformation. However, only a few examples of this kind of political culture improvement can be found. German political parties entered into a 'gentlemen's agreement' before the 2017 election. They stated they would not use leaked information for political purposes, nor use social media bots (Brattberg and Maurer 2018). In Finland, the *education of political parties* is part of a cross-department strategy.[4] The electoral administration under the Ministry

[3] For example, the connection between the far-right United Kingdom Independent Party (UKIP) and the company Cambridge Analytica using big data from Facebook to produce a micro-targeted campaign (see Chapter 2) (Scott 2018).

[4] A so called *whole-of-government approach* also covers the coordination of monitoring, evaluation, and management of hybrid threats. A special government ambassador ensures cooperation between institutions as well as the private sector, and an inter-ministerial group deals with influence operations (Klingová and Milo 2018).

of Justice organised anti-disinformation training for political parties and candidates. Trainings are conducted in various regions so as to be available to everyone. Training should help candidates to recognise and report suspected disinformation and improve their cybersecurity (France 24 2019; KennyBirch 2019).

7.2.6 Direct Countermeasures

We found it necessary to also mention *real time counter-propaganda* as a governmental response. After the poisoning of double agent Sergei Skripal, many European countries expelled their Russian diplomats. This represents a typical example of a direct countermeasure on the state level. No action like this was taken in connection with a hostile propaganda campaign. However, other forms of direct reactions can be identified. French President Macron's IT support, in response to a leaked documents and conversations affair inside his campaign team, fed attackers with bogus information to degrade the value of the leaked content (Brattberg and Maurer 2018; Mohan 2017). This reaction was prepared in advance with campaign staff having anticipated the hacking of their computers; different scenarios were formulated as campaigners realised the threat of interference (EUvsDisinfo 2019).

7.3 Actions of the European Union and NATO

7.3.1 European Union

This is an evolution of the joint approach against disinformation on the EU level; examples of task forces, special bodies countering influence operations, new laws as well as media cooperation can be found. There is a joint task force on the European Union level which was established in 2015. The East StratCom Task Force addresses Russian information campaigns and submits plans for strategic communication. The team consists of staff recruited from EU institutions, or it is seconded by EU member states. The task force's budget exists within the EU budget and those of its member states. (European Union External Action 2018). One of the most visible activities of the task force is the project 'EUvsDisinfo', which 'identifies, compiles, and exposes disinformation cases originating in pro-Kremlin media that are spread across the EU and

Eastern Partnership countries'. The project's current monitoring capabilities 'also uncover disinformation spread in the Western Balkans and the EU's Southern neighbourhood'. The project publishes in 15 languages, updates every week, and distributes a weekly newsletter (EUvsDisinfo, n.d.). In addition to the East StratCom Task Force, the High-Level Expert Group (HLEG) on Fake News and Online Disinformation was established.

An embodiment of these direct countermeasures is one of the Action Plan against Disinformation's pillars: the Rapid Alert System (RAS; European Commission 2019a; European Union External Action 2019). In practice, the RAS should function like an online platform where member states and institutions share their experience and knowledge and prepare common actions. It also aims to cooperate with NATO, the G7, and other partners (European Commission 2019a) The first meeting took place on 18 March 2019, and the RAS has been operational ever since. All member states have designated contact points and institutions (European Parliament 2019a). However, the system needs to be better implemented and tested. There are some critiques about its functioning. For example, Emmott et al. (2019) cites an EU official who stresses that the system is barely used. Kalenský (2019) stresses the problem might be that the RAS is not available to journalists and researchers, so it is not transparent.

When it comes to actions with the media, there is an increasing effort to take the cooperation seriously. Under the Action Plan against Disinformation, the European Union External Action (2018) mobilised an alliance of journalists and fact-checkers with governments, civil society, and academics. The European Union invests in new technologies for content verification (Horizon 2020 programme) and supports the Social Observatory for Disinformation and Social Media Analysis (SOMA), which enables the sharing of best practices among fact-checkers (European Commission 2019a; Emmott et al. 2019). From 18–22 March 2019, the European Commission held Media Literacy Week aiming to 'raise awareness of the importance of media literacy across the EU'. One of the activities was a high-level conference where best practices were presented (European Commission 2019b). Cooperation between the European Union and media companies has occurred with networks such as Facebook, Twitter, and YouTube, including the Code of Practice on Disinformation agreement, published in September 2018 to combat disinformation and fake accounts on their platforms (Emmott et al. 2019). In accordance with the code, Facebook, for example, reported

over 1.2 million actions in the European Union for violation of policies in ads and content. The Code of Practice on Disinformation was built within the context of previous EU initiatives at fighting illegal content, hate speech, and terrorism in the online environment. In May 2016, Facebook, Microsoft, Twitter, and YouTube agreed with the Commission to an EU Code of Conduct on Countering Illegal Hate Speech Online, which set the rules of cooperation and the methodology of content evaluation for countering the spread of illegal hate speech online. In September 2017, the Communication on Tackling Illegal Content Online set other guidelines and principles for collaboration between online platforms, national authorities, member states, and other relevant stakeholders in the fight against illegal content online. In March 2018, the Recommendation on Measures to Effectively Tackle Illegal Online Content focused on calls for proactive measures from providers but also mentioned the importance of human verification. In September 2018, the European Commission proposed the Regulation on the Prevention of the Dissemination of Terrorist Content Online, which contains more restrictive tightening measures against terrorist content, for example, the 'one hour rule' to take terrorist content offline after an order from responsible national authorities (European Parliamentary Research Service 2019).

7.3.2 Nato

On the NATO level, a special initiative called the Strategic Communications Centre of Excellence (Stratcom CoE) has the most visible activities in countering disinformation. Within the NATO structure, it has a specific position and is a NATO-accredited international military organisation. The Centres of Excellence are 'international military organisations that train and educate leaders and specialists from NATO member and partner countries' (NATO Strategic Communications Centre of Excellence 2020a). The institution is not a part of the NATO command structure, nor is it subordinate to another NATO entity. The centre was established after the 2014 Wales Summit, and it aims mostly to contribute to the alliance's strategic communication where research on influence operations and disinformation are included. It also organises conferences and seminars, publishes strategies, and supports NATO exercises (NATO Strategic Communications Centre of Excellence 2020b). As it concerns the cooperation of national governments, 'the decision to join a centre is up to each NATO country. The NATO StratCom Center of Excellence

has fourteen Alliance members, plus the non-NATO countries Sweden and Finland' (Foster 2019). The centre's senior employees consist of Latvian, Estonian, and Polish nationals; other staff hail from the United Kingdom, Belgium, and Germany.

Another significant NATO organisation operating within the topic of cyber and information defence is the NATO Cooperative Cyber Defence Centre of Excellence (The NATO Cooperative Cyber Defence Centre of Excellence 2020). Even though it is more focused on cyber defence, operations in cyberspace, given its complexity, could not be considered without the wider context, where influence operations have irreplaceable positions.

In 2016, the European Centre of Excellence for Countering Hybrid Threats, a joint initiative of the European Union as well as NATO, was established. The centre consists of European Union and NATO member states. The centre aims to be 'an international hub for practitioners and experts' which will assist member states and institutions with hybrid threats defence. It also wants to share practices between states and be a neutral facilitator between the European Union and NATO (The European Centre of Excellence for Countering Hybrid Threats 2019).

7.4 Case Studies

Focused through the analytical framework mentioned above, this chapter illustrates three different approaches to dealing with disinformation and propaganda via three case studies geographically spaced from the western to eastern Europe. This fact is important in the context of the pro-Russian information campaign, which is responsible for one of the biggest shares in spreading disinformation and propaganda in all three countries.

The western case of Denmark reveals a country with a leading position in countermeasures. In central Europe's case, Czech Republic is an example of a country which is 'half-way', with established institutions, international cooperation, and the political will to fight disinformation and propaganda. The last case, from the south-eastern European country of Bulgaria, represents a country which does not have efficient measures.

Of course, this is not an exhaustive list of countries and possible countermeasures. Many other cases could be covered. Nevertheless, we believe these case studies show a wide range of approaches present even in culturally and politically somehow similar countries (at least from a global perspective)—all three countries are members of the European Union

and NATO. However, all three have different approaches to challenging propaganda and disinformation, and it can be seen how different political attitudes, different histories, and different starting positions can affect the approach to countermeasures.

7.4.1 Denmark: Ambitiously Fighting Disinformation

7.4.1.1 Current Situation

Among the threats within the cyber domain, the Danish Defence Intelligence Service (2019) considers Russia, China, Iran, and North Korea as the most active. In comparison to other European states, Denmark is in strong opposition to Russian influence operations. It expelled Russian diplomats after the Skripal affair, and the country was also strongly against the incidents in the Kerch Strait (Scarsi 2019). In hostile disinformation campaigns, Denmark is often framed as a typical Western country in moral decay, especially because of its liberal state model.

In 2018, the Danish government presented 11 initiatives focused on their elections to counter hostile foreign influence. These include a task force, training for communication officers, strengthening the work of intelligence services, emergency preparedness, advising political parties and leaders, dialogue with the media, and updates to its legislation (Ministry of Foreign Affairs of Denmark 2018).

7.4.1.2 Institutional Responses

The Danish Defence Intelligence Service clearly mentioned in its recent annual report, *DDIS Intelligence Risk Assessment 2019*, the threat of Russian cyber and influence operations, which are deployed against well-defined targets. The report also describes China and its cyber and espionage activities with efforts to gather information on an adversary as a threat to Denmark. Clear warning form other state bodies or authorities can also be found (see EUvsDisinfo 2018).

As the European Parliament (2019b) notes, the Ministry of Foreign Affairs is the main safeguard of Danish democracy from foreign influence. In 2019, the ministry launched a strengthened disinformation monitoring programme as a part of the government's new action plan (Ministry of Foreign Affairs of Denmark 2020).

As part of its 11 initiatives, the Danish government launched an interministerial task force to coordinate efforts against disinformation. The ministries are to coordinate together their responses and recognition of

threats (Baumann and Hansen 2017). Denmark considers cyber threats not only disruptions by hostile codes but also influence operations with stress on disinformation and propaganda. The Danish Centre for Cyber Security is a national IT security authority, a network security service, and a national centre for excellence, with a mission 'to advise Danish public authorities and private companies that support functions vital to society on how to prevent, counter and protect against cyber attacks' (Cyber Security Intelligence 2020a; Baumann and Hansen 2017). The centre also considers the role of fake news and social media and covers it in its news analysis (Cyber Security Intelligence 2020b).

Concerning the education of employees, Denmark plans to train communication officers from government authorities on the ongoing handling of disinformation (Ministry of Foreign Affairs of Denmark 2020). An interesting example of this state employee education is the training of Danish soldiers in how to combat disinformation. The plan was a part of NATO's military exercise in Estonia in 2017 (EUvsDisinfo 2017a; Just and Degn 2017). The country intends, in regard to the media, to initiate a dialogue to find models of cooperation (European Parliament 2019b). It is also worth mentioning the documentary *Factory of Lies*, which was aired by the Danish Broadcasting Corporation, exploring the so-called troll farms run by the Kremlin (EUvsDisinfo 2018).

Denmark does not take a strict approach with regard to the regulation of propaganda. The country instead considers it better to strengthen civil society (European Parliament 2019b). When it comes to direct countermeasures, Danish embassy employees are urged to monitor media and mock manipulative stories about Denmark. They were given a great degree of freedom to work offensively at the local and social media level, without the need of coordination from Copenhagen.

Denmark is an active member of the NATO Strategic Communications Centre of Excellence. Cooperation on the supranational level is considered part of its strategy against foreign influence campaigns (The Danish Government 2018). Denmark was one of the actors participating in criticism of the activities of the East StratCom Task Force, especially because of its media categorisation. This event also contributed to questioning Danish membership (for more, see Kulager 2017).

7.4.1.3 Conclusion

Denmark outlined 11 initiatives to fight influence operations covering all aspects. Its approach is aimed more at the role of civil society rather than repressive tools. However, Denmark is very straightforward in naming and warning about adversarial activities. The country has established its own task force and works on inter-ministerial cooperation. It also has a centre focused on cyber threats; however, its approach is more complex and also considers influence operations. Denmark has a great framework as well as plan to deal with hostile propaganda, which could be an inspiration for other European countries. Its implementation is still in its infancy, so the forthcoming years will show its effectivity.

7.4.2 Czech Republic: On the Halfway Mark

7.4.2.1 Current Situation

Czech Republic is currently threatened most by Russian and Chinese intelligence operations, including information warfare (see Security Information Service 2019). There is a large amount of so-called disinformation media with pro-Kremlin sentiments which take information from Russian state sources as well as other disinformation media. Most of these Czech-based platforms, therefore, have no link to the Russian state and instead play the role of sympathisers. Czech Republic, as well as other European states, has become a target of a sophisticated cyber espionage campaign by a hacker group believed to belong to the Russian GRU. In 2019, a cyberattack on the Czech Ministry of Foreign Affairs was revealed to have indicators leading to this group (Lipská 2019). There is also the active role of 'the Castle' in Russian as well as Chinese influence operations, embodied by President Miloš Zeman. He publicly undermines warnings about Russian activities by the Czech Security Information Service (BIS) and plays an important role in disinformation campaigns himself (see Dolejší 2019; Procházková 2018).

7.4.2.2 Institutional Responses

In March 2019, the director of the civil domestic intelligence service BIS, Michal Koudelka, stressed that Russia might interfere, also via a disinformation campaign, in the EU parliamentary election (Kundra 2019; Brolík 2019). Recent annual reports from this service have warned against

Russian secret services and its hybrid strategy to influence decision-making processes as well as Chinese influence actions (Security Information Service 2019). Warnings and statements appear across the political sphere. Minister of the Interior Jan Hamáček (of the Czech Social Democratic Party) warned against disinformation, stressing its importance to Russian President Vladimir Putin, and he recommended citizens check information and discuss it with their relatives (Dragoun 2019). Some opposition parties are also participating in the warning process, albeit with a different discourse. The Civic Democratic Party, for example, emphasised the role of Russia in President Zeman's election and the future threat[5] (see ODS 2018).

The Czech Ministry of Defence also participates in warnings to the public—mostly through individuals though, which is sometimes criticised by the Czech Army itself. General Petr Pavel highlighted the threat from Russia for Czech Republic (iRozhlas 2018). Brigadier General Karel Řehka (2017) wrote a book called *Informační válka* (Information warfare) for academics, the public, and military professionals which is, for example, part of the recommended literature for military courses at the University of Defence.

In 2019, the National Cyber and Information Security Agency (NÚKIB; Národní úřad pro kybernetickou a informační bezpečnost in Czech) published a warning against the use of technologies from Chinese companies Huawei and ZTE (2019a). This warning is also linked to the threat of Chinese influence operations in Czech Republic. The most visible state measure is the Ministry of the Interior's establishment of the Centre Against Terrorism and Hybrid Threats for expert and analytical activities, including disinformation campaigns. The centre is active on Twitter, where it focuses on actual disinformation on the Czech internet (Ministry of the Interior of the Czech Republic 2017). As the centre's head, Benedikt Vangeli, stressed, disproving disinformation includes only about 5–9 per cent of its activities (Janáková 2018). Therefore, we suppose that many of its activities are of a secret nature for a reason. Even though its activities are still not disclosed to public, the centre still functions today.

[5] Contrarywise, the Communist Party is debunking any Russian interference (see KSČM 2017).

The education of employees is manifested through courses for military personnel at the University of Defence, where courses on cyber and information warfare are conducted. NÚKIB organises educational activities for students at universities where it also can recruit its future employees (especially Masaryk University). The agency also organises exercises on cyber and information warfare (11 in 2018), for example, for Czech military personnel, the Czech Integrated Rescue System, and the Czech Statistical Office. NÚKIB describes its activities as an example of whole-of-government, stressing the importance of close cooperation between institutions (National Cyber and Information Security Agency 2019b).

Considering direct countermeasures, it is hard to analyse whether this predominantly covers secret service activities. It is not publicly known if these services are participating in direct information operation activities. However, in 2019, the Cyber and Information Operations Command was established under the Army of the Czech Republic. On its official website, it states that the command will also conduct operations in the information space (Army of the Czech Republic 2019). Even if the description is mostly focused on defensive activities, offensive ones are also relevant to consider.

From interviews with authorities, we can ascertain that Czech Republic is very sensitive to anything concerning free speech and disinformation labelling and may be the reason why the country is careful with content regulation.

On a supranational level, Czech Republic can be considered active and responsible. The country is participating in the East StratCom Task Force. The task force cooperates with the country but also directly with ministries as well as the business sphere. Czech Republic has been a member of the NATO Cooperative Cyber Defence Centre of Excellence since joining in 2018. It actively participates in the centre's activities, achieving, for example, excellent results in cybersecurity exercises. Since 2019, the re-elected EU commissar Věra Jourová gained the values and transparency portfolio also dealing with disinformation. As part of her new mandate, she is working on a new EU action plan where Russia is openly labelled as a threat.[6]

[6] Interview with EU officials.

7.4.2.3 Conclusion

Czech Republic holds a wide spectrum of counter-influence operations activities. Secret services and military officials as well as state authorities emphasise these threats. It is done especially in regard to hostile Russian actions. The country has also established a special body which deals with hybrid threats, unique in the context of central Europe. On the education front, NÚKIB has a role in the education of citizens; however, its focus is mostly on cybersecurity issues. There is no close cooperation or approach with regard to the media and social network providers. Czech Republic actively participates in international cooperation and takes threats from influence operations seriously. Interested state officials often mention an underestimation of strategic communication on the state level as well as its coordination with supranational entities. Together with better implementation into the state education system and amendments to its legal framework, these are the challenges facing the country in the years to come.

7.4.3 Bulgaria: Internal Disunity Through External Influences

7.4.3.1 Current Situation

When speaking about disinformation and propaganda in today's Bulgaria, it is mostly connected with Russian information strategies which try to influence the political orientation of the country from the West to the East, most frequently displayed via disinformation about EU bureaucrats and 'EU bans' on popular food and beverage products (Theresheva 2017). Bulgaria also suspects Russia of supporting anti-migrant vigilantes with equipment and anti-Muslim rhetoric (Fiott and Parkes 2019). One of the most significant connections to the problem of disinformation was the case of leaked documents from the Bulgarian Socialist Party (BSP) (the successor of the Bulgarian Communist Party, see Mavrodieva 2019) which described its strategy for the 2016 presidential election. During the presidential elections, Leonid Reshetnikov, director of the Russian Institute for Strategic Studies, had a meeting with BSP representatives, about the optimisation of their election strategy, where he supposedly instructed BSP on the distribution of fake news and the misinterpretation of election surveys (EUvsDisinfo 2017b). The presidential election was then actually won by BSP candidate Rumen Radev, who is known for his pro-Russian stance (Tsolova 2016). The following section describes the context of

the creation of disinformation and propaganda and the active measures applied against it.

Bulgaria is a specific actor in the question of disinformation and propaganda. On the one hand, it is a member of the European Union and NATO, but it is also, on the other hand, linked to Russia. Disunity in Bulgarian relations to Russia was present in the past and is still present today. You can find here strong pro-Russian tendencies from prominent politicians as well as the presence of anti-Russian discourse. This applies to both the political sphere and to ordinary citizens. One of the latest cases which exacerbated relations between Russia and Europe was the poisoning of the double agent Sergei Skripal and his daughter. Bulgaria was one of the countries which did not expel Russian diplomats as a reaction; the Bulgarian government considered the evidence of Russian involvement in the attack insufficient (de Carbonnel and Tsolova 2018). Citizens also acknowledged this decision. According to a poll, 88 per cent of respondents were against expulsion (Mediapool.bg 2018).

The pro-Russian propaganda channels and instruments are similar to those we know from other European countries, which means using social networks and spreading fake news but also troll farms (Colborne 2018). The main pro-Russian propaganda discourse in Bulgaria concerns European cultural decline under the weight of EU immigration and puppet politics. The European Union is seen as a US-NATO construct, and it is perceived as slowly dying. In contrast, Russia is growing stronger despite Western aggression, especially through adherence to traditional values. Bulgarian civic organisations, non-profit organisations, and the media are then only puppets or foreign agents of the West (Milo et al. 2017). The name George Soros is presented in the country as a sponsor of organisations promoting Western political sentiment in Bulgaria.

7.4.3.2 Institutional Responses

In the category of action with the public and state measures, it is difficult to create countermeasures focused on disinformation coming out of the Russian disinformation strategy because of the division among political elites in relation to the Russian position. The parliament adopted a 2015 report on national security which mentions Russia in the context of its growing military capabilities and the destabilisation of Eastern Ukraine and the countries of the Caucasus, but there is no direct information about a pro-Russian disinformation campaign (BTA 2015). The risk of propaganda and disinformation is not mentioned either in the annual

public reports (SANS 2020) of the State Agency for National Security (SANS) for the years 2016, 2017, and 2018. But in all reports from 2016, there is an unspecified risk for Bulgaria as 'an object of a serious intelligence interest from countries, which view the Union and the Alliance as threats to their own security' (SANS 2016).

There are no specific legal measures, procedures, or laws which were specifically directed against disinformation and propaganda. However, there are law articles connected to the election (see Bayer et al. 2019) which could be potentially used to counter fake news, propaganda, and disinformation as well as regulations concerning the use of campaign finance in electoral codes/acts. For example, Articles 165, 166, and 167 of the 2014 Election Code of Bulgaria define and restrict the amount and sources of money which can be spent on financing election campaigns. Article 168, for its part, states that a party, a coalition, or a nomination committee shall not receive donations from certain sources, such as anonymous donors, legal entities, and religious institutions (Election Code of Bulgaria 2014).

It is additionally difficult to find a direct contribution from Bulgaria on the supranational level. Bulgaria as an EU member state has both information available and the possibility to cooperate in the European External Action Service as well as in the East StratCom Task Force, but there is no evidence that it takes these opportunities. The East StratCom Task Force had pointed out the situation in Bulgaria in several cases. Bulgaria also does not participate in the European Centre of Excellence for Countering Hybrid Threats (2019).

Unfortunately, there are no signs of state activity with the media, political parties, or in direct countermeasures.

7.4.3.3 Conclusion

Bulgaria is an example of a country which, despite having international cooperation with the European Union and NATO and their member states, has very limited active measures against propaganda and disinformation. The key element of this is the relationship of some Bulgarian political actors to Russia. This example shows that disinformation and propaganda are highly politicised issues, and, without the support of local political elites, efforts from the international level are inefficient. In this case, all measures targeting pro-Russian disinformation are problematic, but there is still a place for measures focused more broadly—on election campaigns in general, corruption, and so forth.

It is possible that with stronger pressure from the Russian side, it will be easier to find the political will for a clear stance against disinformation. Expelling Russian diplomats in January 2020 over espionage allegations in October 2019 and declining to grant a visa to an incoming Russian defence attaché may possibly cause the situation to reverse. The relationship between Bulgaria and Russia may be worsened by the fact that Bulgarian prosecutors charged three Russians with the attempted murder of an arms trader and two other Bulgarians whose poisoning is being investigated by Sofia for possible links with the 2018 nerve-agent attack on Skripal (Reuters 2020).

7.5 Conclusion

The approach of European national institutions to disinformation and propaganda covers a wide spectrum of countermeasures. Together, it is possible to formulate a joint framework and apply it to specific actors to evaluate its capabilities. Denmark, Czech Republic, and Bulgaria were chosen because of their different states of countermeasure development to disinformation and propaganda. This approach should help to better understand the issues in the fight against disinformation and present the application of the proposed framework in practice.

Seven categories of state institutional responses against disinformation and propaganda have been formulated. The first group of countermeasures are *actions with the public* and *state measures*, which cover the most common countermeasures in Europe, and it is possible to identify them in all our cases. The second group of countermeasures are *legal measures*, *actions with the media*, and *actions with political parties*. These are more complex and demand processed legislation and a long-term coherent strategy. For these reasons, we can see these countermeasures in countries which are leading the development of measures against disinformation, such as in Finland or Denmark. The final categories are *direct countermeasures* and *actions with supranational entities*. They are the most problematic due to a lack of public information concerning them. These categories are closely connected with security services and diplomacy, and we can only identify public acts, such as the expulsion of diplomats or public initiatives in international organisations like NATO or the European Union.

All in all, this chapter introduces an analytical framework in which to analyse a set of countermeasures against disinformation as part of influence operations, and it has given the researcher the opportunity to depict the issue in its complexity and, therefore, to study the strengths and weaknesses of the system. The analytical framework and its usage were demonstrated on a limited scale. More detailed research is recommended, specifically in the collection of data through the use of interviews with political campaign managers, specialists, high-level state authorities, and experts.

Bibliography

Algemene Inlichtingen- en Veuligheidsdiest. Ministerie Binnenlandse Zaken en Koninkrijksrelaties. (2018). Spionage en ongewenste inmenging. *Report*. https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2018/spionage. Accessed 15 Nov 2019.

Army of the Czech Republic. (2019). *Velitelství kybernetických sil a informačních operací* [Chief of Cyber and Information Operations]. http://www.acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/. Accessed 15 Nov 2019.

Baumann, A., & Hansen, A. R. (2017, September 10). *Danmark får ny kommandocentral mod misinformation*. https://www.mm.dk/tjekdet/artikel/danmark-faar-ny-kommandocentral-mod-misinformation. Accessed 15 Nov 2019.

Bayer, J., et al. (2019). *Disinformation and Propaganda—Impact on the Functioning of the Rule of Law in the EU and Its Member States*. Policy Department for Citizens' Rights and Constitutional Affairs. http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf. Accessed 15 Nov 2019.

Bleiker, C., & Brady, K. (2017, June 30). Bundestag Passes Law to Fine Social Media Companies for Not Deleting Hate Speech. *Deutsche Welle*. https://www.dw.com/en/bundestag-passes-law-to-fine-social-media-companies-for-not-deleting-hate-speech/a-39486694. Accessed 15 Nov 2019.

Brattberg, E., & Maurer, T. (2018). *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. 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. Accessed 15 Nov 2019.

Brolík, T. (2019, May 3). Šéf BIS: Rusko se nám pokusí vměšovat do voleb [Director of Security Intelligence Service: Russia Will Try to Meddle into

Our Elections]. *Respekt*. https://www.respekt.cz/politika/sef-bis-rusko-se-u-nas-pokusi-vmesovat-do-eurovoleb. Accessed 15 Nov 2019.

BTA. (2015, September 1). Parliament Adopts Report on National Security in 2015. *Bulgarian News Agency*. http://www.bta.bg/en/c/DF/id/1408996. Accessed 15 Nov 2019.

Charlton, E. (2019, May 21). How Finland Is Fighting Fake News—In the Classroom. *World Economic Forum*. https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom. Accessed 15 Nov 2019.

Cheresheva, M. (2017, December 12). False Reports of EU Bans InflameBulgarians. *Balkan Insight*. https://balkaninsight.com/2017/12/12/myths-about-tough-eu-bans-scare-bulgarians-12-11-2017/. Accessed 15 Nov 2019.

Colborne, M. (2018, May 9). Made in Bulgaria: Pro-Russian Propaganda. *Coda Story*. https://codastory.com/disinformation-crisis/foreign-proxies/made-in-bulgaria-pro-russian-propaganda. Accessed 15 Nov 2019.

Cyber Security Intelligence. (2020a). https://www.cybersecurityintelligence.com/centre-for-cyber-security-cfcs-3071.html. Accessed 4 Mar 2020.

Cyber Security Intelligence. (2020b). *Publishers Spread Fake News*. https://www.cybersecurityintelligence.com/blog/publishers-spread-fake-news–4756.html. Accessed 4 Mar 2020.

Danish Defence Intelligence Service. (2019). Intelligence Risk Assessment 2019. *An Assessment of Developments Abroad Impacting on Danish Security*. https://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Intelligence%20Risk%20Assessment%202019.pdf. Accessed 15 Nov 2019.

de Carbonnel, A., & Tsolova, T. (2018, March 29). Old Ties with Russia Weigh on Bulgarian Decision in Spy Poisoning Case. *Reuters*. https://www.reuters.com/article/us-britain-russia-bulgaria/old-ties-with-russia-weigh-on-bulgarian-decision-in-spy-poisoning-case-idUSKBN1H52BR. Accessed 15 Nov 2019.

Denmark Ministry of Foreign Affairs. (2018, September 7). The Danish Government Presents a Plan with 11 Initiatives Aimed at Strengthening Danish Resilience Against Influence Campaigns. *Twitter*. https://bit.ly/2HV3ja1. Accessed 15 Nov 2019.

Dolejší, V. (2019, May 8). CIA mu dala cenu, Zeman označil za „čučkaře“. Proč šéfa BIS už potřetí nejmenuje prezident generálem [He Was Awarded by CIA, Zeman Labelled Him as Amateur. Why the Director of the Security and Information Service Will Not Be Promoted for the Third Time to General]. *Seznam zprávy*. https://www.seznamzpravy.cz/clanek/cia-mu-dala-cenu-zeman-oznacil-za-cuckare-proc-sefa-bis-uz-potreti-nejmenuje-prezident-generalem-71687. Accessed 15 Nov 2019.

Dragoun, R. (2019, May 3). Hamáček varoval před dezinformacemi. Eurovolby jsou pro Putina klíčové, říká analytic [Hamáček Warned Against Disinformation. Analyst Says That European Elections Are Crucial for Putin]. *Aktualne.cz*. https://zpravy.aktualne.cz/zahranici/evropsky-parlament/volby-budou-cilem-dezinformatoru-varoval-hamacek/r~5dd9119e6d8e11e9b2a00cc47ab5f122/. Accessed 15 Nov 2019.

Election Code of Bulgaria. (2014). https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2014)025-e. Accessed 15 Nov 2019.

Emmott, R., Carbonnel, A., & Humphries, C. (2019, March 16). Who Burnt Notre Dame? Brussels Goes After Fake News as EU Election Nears. *Reuters*. https://ru.reuters.com/article/worldNews/idUKKCN1SM0LA. Accessed 15 Nov 2019.

Estonian Foreign Intelligence Service. (2019). *International Security and Estonia 2019*. https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf. Accessed 15 Nov 2019.

EU Observer. (2019, March 13). *Estonian Spies Warn EU on Russian Security Threat*. https://euobserver.com/foreign/144389. Accessed 15 Nov 2019.

European Commission. (2019a). Action Plan Against Disinformation. *Report on Progress*. https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf. Accessed 15 Nov 2019.

European Commission. (2019b). *European Media Literacy Week*. https://ec.europa.eu/digital-single-market/en/news/european-media-literacy-week. Accessed 15 Nov 2019.

European Parliament. (2019a). *Answer Given by Vice-President Mogherini on Behalf of the European Commission*. http://www.europarl.europa.eu/doceo/document/P-8-2019-001705-ASW_EN.html. Accessed 15 Nov 2019.

European Parliament. (2019b). Automated Tackling of Disinformation. Panel for the Future of Science and Technology European Science-Media Hub. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf. Accessed 15 Nov 2019.

European Parliamentary Research Service. (2019). *Regulating Disinformation with Artificial Intelligence*. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf. Accessed 15 Nov 2019.

European Union External Action. (2018). *Questions and Answers About the East StratCom Task Force*. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en. Accessed 15 Nov 2019.

European Union External Action. (2019). *Factsheet: Rapid Alert System*. https://eeas.europa.eu/headquarters/headquarters-Homepage_en/59644/Factsheet:%20Rapid%20Alert%20System. Accessed 15 Nov 2019.

EUvsDisinfo. (2017a, July 25). *Denmark to Educate Soldiers in Combatting Disinformation*. https://euvsdisinfo.eu/denmark-to-educate-soldiers-in-combatting-disinformation/. Accessed 15 Nov 2019.

EuvsDisinfo. (2017b, March 28). *Fake News and Elections in Bulgaria*. https://euvsdisinfo.eu/fake-news-and-elections/. Accessed 15 Nov 2019.

EUvsDisinfo. (2018, September 10). *Denmark's Defence Against Disinformation*. https://euvsdisinfo.eu/denmarks-defence-against-disinformation/. Accessed 15 Nov 2019.

EUvsDisinfo. (2019, May 6). *Tackling disinformation à la française*. https://euvsdisinfo.eu/tackling-disinformation-a-la-francaise/. Accessed 15 Nov 2019.

EUvsDisinfo. (n.d.). *About*. https://euvsdisinfo.eu/about/. Accessed 15 Nov 2019.

Facebook. (2019). *Community Standards: False News*. https://www.facebook.com/communitystandards/false_news. Accessed 15 Nov 2019.

Facebook. (2020). *Fact-Checking on Facebook: What Publishers Should Know*. https://www.facebook.com/help/publisher/182222309230722. Accessed 15 Nov 2019.

Fiott, D., & Parkes, R. (2019). *Protecting Europe: The EUs Response to Hybrid Threats*. Paris: European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf. Accessed 15 Nov 2019.

Flamini, D., & Tardáguila, C. (2019). *A First Look at the OAS's Recommendations for Best Practices Against Electoral Misinformation, Part 2*. https://www.poynter.org/fact-checking/2019/a-first-look-at-the-oass-recommendations-for-best-practices-against-electoral-misinformation-part-2/. Accessed 15 Nov 2019.

Foster, H. (2019). *#StrongerWithAllies: Meet the Latvian Who Leads NATO's Fight Against Fake News*. Washington: Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/strongerwithallies-latvian-leads-nato-s-fight-against-fake-news/. Accessed 15 Nov 2019.

France 24. (2019, April 13). *Election Ads Urge Finns 'Think for Yourself' Amid Fake News Fears*. https://www.france24.com/en/20190413-election-ads-urge-finns-think-yourself-amid-fake-news-fears. Accessed 15 Nov 2019.

Google. (2019). *How Google Fights Disinformation*. https://kstatic.googleusercontent.com/files/388aa7d18189665e5f5579aef18e181c2d4283fb7b0d4691689dfd1bf92f7ac2ea6816e09c02eb98d5501b8e5705ead65af653cdf94071c47361821e362da55b. Accessed 15 Nov 2019.

Hanzelka, J., & Kasl, F. (2018). Sekuritizace a právní nástroje pro boj s projevy nenávisti na internetu v Německu [Securitization and Legal Instruments for Countering Cyber Hate in Germany]. *Acta Politologica*, *10*(3), 20–46. https://doi.org/10.14712/1803-8220/15_2018.

Interfax-Ukraine. (2014). *Poroshenko: Information Ministry's Main Task Is to Repel Information Attacks Against Ukraine*. https://en.interfax.com.ua/news/economic/238615.html. Accessed 15 Nov 2019.

iRozhlas. (2018, November 8). *Petr Pavel: Aktivity Ruska jsou pro Česko větší hrozba než terorismus* [Petr Pavel: Russian Activities Are for the Czech Republic More Serious Threat Than Terrorism]. https://www.irozhlas.cz/zpravy-domov/petr-pavel-rusko-hrozba-nato_1811081818_cen. Accessed 15 Nov 2019.

Janáková, B. (2018, March 23). Centrum proti terorismu vyvrátilo za rok 22 dezinformací. Má i jiné úkoly [Centre Against Terrorism Debunked 22 Disinformation in the Las Year. It Has Also Other Tasks]. *Idnes*. https://www.idnes.cz/zpravy/domaci/dezinformace-hoaxy-fake-news-centrum-proti-terorismu-a-hybridnim-hrozbam-cthh-ministerstvo-vnitra-lu.A180314_105400_domaci_bja. Accessed 15 Nov 2019.

Just, A. N., & Degn, S. F. (2017, July 17). Danske soldater skal beskyttes mod fake news fra Rusland. *DR*. https://www.dr.dk/nyheder/politik/danske-soldater-skal-beskyttes-mod-fake-news-fra-rusland. Accessed 15 Nov 2019.

Kalenský, J. (2019). *Evaluation of the EU Elections: Many Gaps Still Remain. Disinfo Portal*. https://disinfoportal.org/evaluation-of-the-eu-elections-many-gaps-still-remain/. Accessed 15 Nov 2019.

KennyBirch, R. (2019, December 3). How Finland Shuts Down Fake News. *Apolitical*. https://apolitical.co/en/solution_article/how-finland-shuts-down-fake-news. Accessed 15 Nov 2019.

Klingová, K., & Milo, D. (2018). *Boj proti hybridným hrozbám v krajinách EÚ: príklady dobrej praxe* [Fight Against Hybrid Threats in EU Countries: Good Practice Examples]. Bratislava: GLOBSEC. Accessed 15 Nov 2019.

Kremlin Watch. (2020). Belgium. *Counties Compared*. https://www.kremlinwatch.eu/countries-compared-states/belgium/. Accessed 15 Nov 2019.

KSČM. (2017). *Ovlivnila hybridní válka o lithiové baterie volby? Konspirační teorie versus fakta* [Did Hybrid War on Lithium Batteries Affected Elections? Conspiracy Theory Versus Facts]. https://www.kscm.cz/cs/aktualne/medialni-vystupy/komentare/ovlivnila-hybridni-valka-o-lithiove-baterie-volby-konspiracni. Accessed 15 Nov 2019.

Kulager, F. (2017, April 17). Informationskrigen under lup: Sådan spreder Ruslands dagsorden sig i Danmark. *Zetland*. https://www.zetland.dk/historie/sOXVEKv3-aOZj67pz-3bd93. Accessed 15 Nov 2019.

Kundra, O. (2019, March 13). Ředitel BIS: Rusko má zájem ovlivnit evropské volby [Director of the Security and Information Service: Russia Has Interest to Influence European Elections]. *Respekt*. https://www.respekt.cz/politika/bis-evropske-volby. Accessed 15 Nov 2019.

Lipská, J. (2019, August 13). Byl to útok cizí státní moci, uvedl NÚKIB k napadení serverů ministerstva zahraničí [National Cyber Authority Says About

Cyber Attack on Ministry of Foreign Affairs: It Was Attack of Foreign State Actor]. *Seznam zprávy*. https://www.seznamzpravy.cz/clanek/byl-to-utok-cizi-statni-moci-rekl-nukib-k-napadeni-serveru-ministerstva-zahranici-77215. Accessed 15 Nov 2019.

Mackintosh, E., & Kiernan, E. (2019, May 18). Finland Is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy. *CNN*. shorturl.at/clFX4. Accessed 15 Nov 2019.

Marsden, C., & Meyer, T. (2019). *Regulating Disinformation with Artificial Intelligence*. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf. Accessed 15 Nov 2019.

Mavrodieva, I. (2019). Bulgaria. In O. Eibl & M. Gregor (Eds.), *Thirty Years of Political Campaigning in Central and Eastern Europe*. London: Palgrave.

Media Animation ASBl. (2020). https://media-animation.be/. Accessed 3 Mar 2020.

Mediapool.bg (2018, April 6). Проучване: Българите са солидарни с Русия по случая "Скрипал". *Mediapool*. https://www.mediapool.bg/prouchvane-balgarite-sa-solidarni-s-rusiya-po-sluchaya-skripal-news277716.html. Accessed 15 Nov 2019.

Milo, D., Klingová, K., & Hajdu, D. (2017). *GLOBSEC Trend 2017: Mixed Messages and Signs of Hope from Central & Eastern Europe*. Bratislava: GLOBSEC Policy Institute. https://www.globsec.org/wp-content/uploads/2017/09/globsec_trends_2017.pdf. Accessed 15 Nov 2019.

Ministry of Foreign Affairs of Denmark. (2020). *Strengthened safeguards against foreign influence on Danish elections and democracy*. https://um.dk/en/news/newsdisplaypage/?newsid=1df5adbb-d1df-402b-b9ac-57fd4485ffa4.

Ministry of Information Policy of Ukraine. (2018). *Bila kniga specialnih informacijnih operacij proti Ukraïni 2014–2018*. https://mip.gov.ua/files/pdf/white_book_2018_mip.pdf. Accessed 15 Nov 2019.

Ministry of Interior of the Czech Republic. (2017). *Centre Against Terrorism and Hybrid Threats*. https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx. Accessed 15 Nov 2019.

Mohan, M. (2017, May 9). Macron Leaks: The Anatomy of a Hack. *BBC*. https://www.bbc.com/news/blogs-trending-39845105. Accessed 15 Nov 2019.

National Cyber and Information Security Agency. (2019a). Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou [Huawei and ZTE Software and Hardware Are Security Threat]. https://www.govcert.cz/cs/informacni-servis/hrozby/2680-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/. Accessed 15 Nov 2019.

National Cyber and Information Security Agency. (2019b). *Report on the State of Cyber Security in the Czech Republic in 2018*. https://www.nukib.cz/cs/informacni-servis/publikace/. Accessed 15 Nov 2019.

NATO Strategic Communications Centre of Excellence. (2020a). *FAQ*. https://www.stratcomcoe.org/faq. Accessed 15 Nov 2019.

NATO Strategic Communications Centre of Excellence. (2020b). *About Us*. https://www.stratcomcoe.org/about-us. Accessed 15 Nov 2019.

ODS. (2018). Alexandra Udženija: Respekt k výsledku voleb přece neznamená, že mají lidé mlčet [Alexandra Udženija: Respect to the Election Results Does Not Mean That People Should Be Silent]. https://www.ods.cz/clanek/16828-respekt-k-vysledku-voleb-prece-neznamena-ze-maji-lide-mlcet. Accessed 15 Nov 2019.

Press TV. (2017, February 28). *Germany to Help Baltic States Establish Russian-Language Media*. https://www.presstv.com/Detail/2017/02/28/512397/Germany-Russianlanguage-media-Baltic-states. Accessed 15 Nov 2019.

Procházková, P. (2018, October 17). Výrok prezidenta Zemana o Novičoku se stal samostatnou kapitolou v Kapesním průvodci po ruské propagandě [Comments of President Zeman About Novichok Has Become New Chapter in Pocket Guide in Russian Propaganda]. *Nový deník*. https://denikn.cz/1864/prezident-zeman-se-stal-samostatnou-kapitolou-v-kapesnim-pruvodci-po-ruske-propagande/. Accessed 15 Nov 2019.

Řehka, K. (2017). *Informační válka* [Information War]. Praha: Academia.

Reuters. (2020, January 24). *Bulgaria Expels Two Russian Diplomats for Espionage*. https://www.reuters.com/article/us-bulgaria-russia/bulgaria-expels-two-russian-diplomats-for-espionage-idUSKBN1ZN10K. Accessed 17 Feb 2020.

Robinson, O., Coleman, A., & Sardarizadeh, S. (2019). *A Report of Anti-Disinformation Initiatives*. Oxford Technology and Election Commission. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/08/A-Report-of-Anti-Disinformation-Initiatives. Accessed 15 Nov 2019.

Roden, L. (2017, March 13). Swedish Kids to Learn Computer Coding and How to Spot Fake News in Primary School. *The Local*. https://www.thelocal.se/20170313/swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school. Accessed 15 Nov 2019.

Rozgonyi, K. (2018). *The Impact of the Information Disorder (Disinformation) on Election*. European Commission for Democracy Through Law. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-LA(2018)002-e. Accessed 15 Nov 2019.

SANS. (2016). *Annual Report 2016*. State Agency for National Security. http://www.dans.bg/images/stories/Information/Doklad_DANS_2016_en.pdf. Accessed 15 Nov 2019.

SANS. (2020). *Annual Reports*. State Agency for National Security. http://www.dans.bg/en/report-23012018-sec-en. Accessed 21 Feb 2020.

Scarsi, A. (2019, January 29). Denmark Calls on EU to Act Against Putin: Copenhagen FURY at Russia 'Aggressive Behaviour'. *Express*. https://bit.ly/2UbQqPF. Accessed 15 Nov 2019.

Scott, M. (2018, June 30). Cambridge Analytica Did Work for Brexit Groups, Says Ex-staffer. *Politico*. https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/. Accessed 15 Nov 2019.

Security Information Service. (2019). *Annual Report of the Security Information Service*. https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2018en.pdf.pdf. Accessed 15 Nov 2019.

Sternstein, A. (2017). *Estonia's Lessons for Fighting Russian Disinformation*. https://www.csmonitor.com/World/Passcode/2017/0324/Estonia-s-lessons-for-fighting-Russian-disinformation. Accessed 15 Nov 2019.

Stone, J. (2019, May 20). Austrian Government Cannot Be Trusted with Intelligence Due to Far-Right Links, German Security Service Warns. *Independent*. https://www.independent.co.uk/news/world/europe/austria-germany-intelligence-security-services-russia-bfv-a8921966.html. Accessed 15 Nov 2019.

Swedish Civil Contingencies Agency. (2018). *If Crisis or War Comes*. http://www.documentcloud.org/documents/4481608-Om-Krisen-Eller-Kriget-Kommer-Engelska.html#document/p1. Accessed 15 Nov 2019.

Swedish Civil Contingencies Agency. (2019). *Countering Information Influence Activities: A Handbook for Communicators*. https://www.msb.se/RibData/Filer/pdf/28698.pdf. Accessed 15 Nov 2019.

The Danish Government. (2018). *Denmark Foreign and Security Policy Strategy 2019–2020*. https://www.dsn.gob.es/sites/dsn/files/2018_Denmark%20Foreign%20and%20security%20policy%20strategy%202019-2020.pdf. Accessed 15 Nov 2019.

The European Centre of Excellence for Countering Hybrid Threats. (2019). *Joining Dates of the Hybrid CoE Member States*. https://www.hybridcoe.fi/wp-content/uploads/2019/12/Joining-Dates-Alfabetic-Order-1.pdf. Accessed 3 Feb 2020.

The NATO Cooperative Cyber Defence Centre of Excellence. (2020). https://ccdcoe.org/about-us/. Accessed 15 Nov 2019.

Tsolova, T. (2016, November 11). Bulgarian Vote Shows Russia Winning Hearts on EU's Eastern Flank. *Reuters*. https://www.reuters.com/article/us-bulgaria-election-russia/bulgarian-vote-shows-russia-winning-hearts-on-eus-eastern-flank-idUSKBN13611H. Accessed 15 Nov 2019.

Ukrainian Independent Information Agency of News. (2019, February 12). *Ukraine's Ministry of Information Policy Presents "White Book" of Info-ops Against Ukraine*. https://www.unian.info/politics/10443192-ukraine-s-ministry-of-information-policy-presents-white-book-of-info-ops-against-ukraine.htm. Accessed 15 Nov 2019.