STRATPOL
Strategic Policy Institute

Policy Paper

Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns

Asya Metodieva[1]

Executive summary

Disinformation campaigns have become a considerable threat to domestic political processes across Europe. The 2017 French and German elections testified to Russian efforts to meddle in domestic political affairs. The Visegrad states have also been targets of extensive disinformation campaigns following the annexation of Crimea in 2014. The pro-Kremlin disinformation strategy in Central Europe weakens the West while strengthening the Russian political influence on the region. This policy brief discusses information warfare threats to the Czech Republic, Hungary, Poland and Slovakia and evaluates their state-level strategic responses. The paper specifically focuses on pro-Russian disinformation activities as a form of cyber-threat. It argues that while some Visegrad states securitize the issue at the political level, other offer an environment conducive to online propaganda simply because they do not consider it a problem. At least three factors contribute to the cyber-security behaviour of the Visegrad states: 1) Capacity to react, 2) Political regime change and 3) Relationship with Russia. This analysis aims to provide local governments with a comprehensive overview of the V4 cyber-security landscape, help them improve their national policies and deepen regional cooperation.

Keywords: V4, Cyber security, Disinformation, Cyber defence, Cyber capabilities

[1]Asya Metodieva is a PhD Candidate at the Central European University (CEU), Budapest. She holds MA in International Public Policy from CEU and MA in International Relations and Security Studies from Sofia University "St. Kliment Ohridski". Her research interests include Global Governance, International Security (Terrorism and Counter-Terrorism, Energy Security, Cyber Security), and Politics of Central and Eastern Europe. Her research is on foreign fighter mobilization in post-violent societies with a focus on the Western Balkans. Previously, Asya worked as a journalist for the Bulgarian National Television.

© 2018 · STRATPOL · office@stratpol.sk · +421 908 893 424 · www.stratpol.sk

Recommendations

At the national level, V4 governments need to:

- Come up with more precise definitions of cyber-security threats and make them available to a broad circle of stakeholders, including media and private companies;
- Introduce concrete measures addressing disinformation campaigns and make them available to a broad circle of stakeholders, including media and private companies;
- Publish annual reports on cyber incidents through the institutions responsible for collecting such data;
- Better cooperation with the private and civil sectors;
- Make clear that both private companies and civil society groups are desirable and necessary partners in the field of cyber-security due to their expertise and capacity to address new threats.
- Encourage telecom operators and other private actors to improve their cyber-security capacities and invest in future digital infrastructure (Fiber, Cloud, and 5G).

At the regional level, V4 governments need to:

- Build general awareness of disinformation threats by introducing joint standards in defining cyber threats; this can boost the general public's resilience against such campaigns.
- Discuss national-level incidents within the V4 format;
- Organize regional conferences on the issue of disinformation campaigns;
- Cooperate at the academic level that will enhance the chance for accessing funding for region research projects in cyber-security.
- Create possibilities for regional cooperation among national authorities responsible for cyber-security;
- Build on the Central European Cyber Security Platform and develop further regional partnerships with potential V4+ partners;
- Conduct annual comparative reviews of the national cyber-security strategies and their implementation;
- Learn from the experience of the other countries in the region. The Czech Republic has developed valuable expertise in dealing with disinformation campaigns. The state demonstrates successful strategic and policy shifts and good practices in cyber-security tasks' distribution. Its relatively decentralized model of institutional infrastructure can be easily adopted by the other Visegrad states. Poland, on the other hand, has the capacity to incentivize further regional cooperation due to the size of its economy and the emphasis that the country puts on cyber-security.

Cyber-security: What is it all about?

Cyber-attacks are among the most challenging threats to national and international security. They may come in various forms – from disinformation campaigns to hostile operations on critical infrastructure. The proliferation of cyber-warfare creates new security challenges that require an arsenal of new military, organizational and legal responses. The concept of cyber-security emerges from the relationship between technological advancement and new geopolitical conditions in the post-Cold War period (Hansen and Nissenbaum 2009). It refers to potential technology-based threats to a society (Nissenbaum 2005). Almost three decades ago, Ulrich Beck (1992) anticipated in his "risk society" theory that interconnectedness between systems in the modern society increases the possibility of new hazards. Hardt and Negri (2004) emphasize that only a power in a network can maintain order nowadays. They describe the contemporary security environment as "a state of war in which network forces of imperial order face network enemies on all sides" (Hardt and Negri 2004).

The latest wave of policy research on cyber-security addresses two broad topics: 1) the role of social media and 2) vulnerabilities of critical infrastructure that leave space for cyber-attacks.

Social media platforms have become not only channels for exchanging political ideas and attitudes, but also venues for manipulative disinformation campaigns (Woolley and Howard 2017). Political actors have employed bots and trolls to purposefully disseminate misleading information and shape public opinion (Forelle et al. 2015, Gallacher et al 2017, Woolley and Howard 2017). Recent election campaigns in Europe and in the US[2] have illustrated how social media bots, and computational propaganda more broadly, influence online discussions (Woolley and Howard 2017). Political bots, organized trolling, campaigns of hate and harassment and "fake news" are the most distinctive forms of computational propaganda (Gorwa 2017).

Table 1: Key terminology of disinformation

Bots	Software created to perform simple, repetitive, robotic tasks, and thus, they can easily spread propaganda. Social media bots function as automated identities (they look and act online like real users) that can collect information and communicate with people and systems (Woolley and Howard 2017).
Trolling	Activity of online users, who intentionally post comments on articles; write posts on social media in an attempt to influence political and civil society's discussions on the Internet. These "cyber mercenaries" (Maurer 2017) are sometimes paid by political actors to silence opponents or protesting groups. Adrian Chen's 2015 journalistic investigation has revealed the existence of a "troll-factory" in Russia with hundreds of employees paid to disrupt online discussions. This type of organization is also known as a "troll-farm" or a "troll-army" (Gorwa 2017).

[2] 2017 French presidential election, 2017 German federal election, 2018 Czech presidential election, 2016 US presidential election, etc.

"Fake news"	A term born with the beginning of Donald Trump's presidency. Generally, it refers to "intentionally incorrect or misleading information spread by a news organization (real or not) for political purposes" (Gorwa 2017).

All these forms of computational propaganda may be separate elements of a more comprehensive disinformation campaign. They are usually employed by politicians, parties, and lobby groups to push political agendas, attack opponents, journalists, activist groups (Woolley and Howard 2017).

Cyber-attacks on critical infrastructure (not in the focus of this paper) have inspired another broader body of cyber-security research, as well as latest updates on national and international strategic documents. To be considered a critical infrastructure, an element or a system of infrastructure must fulfil one of the criteria on significant casualties, economic effects, or public effects (EU Council Directive 2008/114/EC). Critical infrastructure usually refers to the communication and information systems in sectors such as transport, energy, emergency services, health services, water management, food industry and agriculture, communication systems, financial markets and public administration (Minarik 2016).

At a policy level, cyber-security is a horizontal policy (Botond Feledy 2017). It involves a wide variety of stakeholders, including national and international institutions, public and private actors. Differences in political agendas and technological developments at the national level lead to the different prioritization of cyber-security threats (Hare 2010). In other words, it matters how policy-makers define cyber-threats and how equipped they are to counter them. The EU-level legal framework is one of the key driving forces behind the development of national cyber-structures across Europe (Botond Feledy 2017). The General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive) are the two legal fundaments in this field. Among the recent documents of high relevance lies the conclusion of the European Digital Summit in Tallinn. It suggests that Europe will be "a global leader in cyber-security by 2025" (Tallinn Digital Summit 2017). Although the European Commission set a goal in 2015 to complete the Digital Single Market by the end of 2018, finalizing the process within the next six months is unlikely. Moreover, the current European cyber-security landscape remains fragmented due to variations in administrative cultures and clashing political interests at the national level (Botond Feledy 2017). This fragmentation creates space for external malicious actors.

In all four Visegrad states (V4), cyber-security is a strategic element of their national security agendas. Nonetheless, the four differ in their threat definitions, distribution of cyber-security tasks within national security infrastructures; stakeholder involvement and capacity to invest in expertise and new technological solutions. As the analysis is specifically concerned with pro-Russian disinformation campaigns, it looks at three factors, contributing to the cyber-security behaviour of the Czech Republic, Hungary, Poland, and Slovakia: 1) Capacity to react, 2) Political regime change and 3) Relationship with Russia.

The paper offers a comprehensive overview of the V4 national approaches to cyber-security including threats and responses, political and strategic organization, legislation and distribution of cyber-security tasks among the different agencies at the national level. The reviewed sources include reports of the NATO Cooperative Cyber Defence Centre of Excellence, national strategic and policy documents, an overview of counter-measures by the V4 to Russian disinformation operations, and other reports produced by local and international research institutions. First, the paper looks separately at each country's approach to cyber-security. It then examines the political regime change as a factor with possible implications for national cyber-security policies. Finally, it analyses whether the Visegrad states consider the pro-Kremlin disinformation campaigns a security threat to their national security landscapes, and if so, how they respond. The paper offers conclusions and policy recommendations that may help the Visegrad states improve their national policies and deepen regional cooperation.

Capacity to react: National Cyber-Security Strategies and Organizations of the V4 states

The key strategic documents of the Czech Republic, Hungary, Poland and Slovakia acknowledge that the international security environment has become highly unpredictable in the past years. Without exception, the reviewed documents consider a threat the aggressive promotion of foreign-policy interests of third states by means of technology (Necej and Zilincik 2017). While most documents list hybrid activities and hostile cyber operations among other security threats, they do not necessarily specify disinformation campaigns. At the same time, the Visegrad states struggle to keep up with the newest technologies and establish adequate national cyber-security institutions.

Czech Republic

At the strategic level, The Czech National Cyber Security Strategy (NCSS) and the associated Action Plan (2015-2020) are the key documents concerned with cyber-security. They suggest that the Czech Republic will play "a leading role" in this field within the region, more broadly in Europe (NCSS 2015-2020). Cyber-security is also a matter in other strategic documents, such as the Security Strategy of the Czech Republic (2015) and the Long-Term Perspective for Defence 2030 (2015). The Act on Cyber Security and Change of Related Acts, which took effect in January 2015, is the legal cyber-security framework. The Czech legislation introduces the concept of a limited state of emergency known as a "state of cyber emergency" (Act No. 181/2014 Coll.). It can be declared when the national interest is threatened by a danger to information security or to the security of communications services (Minarik 2016).

At the organizational level, the main coordinating body is the National Cyber and Information Security Agency (NÚKIB, within the NSA-Czech Republic) tasked with general cyber-security protection. The body in charge for civilian cyber-monitoring/capabilities is the Centre against Terrorism and Hybrid Threats. It specifically deals with disinformation

campaigns, among other tasks. This unit was established following recommendations of the 2016 National Security Audit. Government CERT (GovCERT.cz) and other CSIRT teams play a key role in safeguarding the critical information infrastructure. They collect reports of cyber incidents, analyse them and provide support. The body tasked with military cyber-monitoring is the Communications and Information Systems Agency (CISA). The National Cyber Forces Centre (NCFC), within the Military Intelligence, is another unit expected to be fully operational in 2020 (Minarik 2016). The intelligence agency with cyber-capabilities is the Security Information Service (BIS), which is also the key national intelligence institution. It is responsible for the collection and evaluation of data concerning national security. Regarding NATO CCD COE/STRATCOM bodies and activities, the Czech Republic participates in EEAS East STRATCOM Team (Brussels) and NATO STRATCOM COE (Latvia) (Janda et. al. 2017). It also takes part in NATO Cyber Coalition and NATO Crisis Management Exercises.

Hungary

At the strategic level, the National Cyber Security Strategy of Hungary (2013) is the key document concerned with cyber-security. The document promises active cooperation between state and non-state actors, military and law enforcement, economic and political stakeholders (Kovacs and Szentgali 2015). Cyber-security is also a matter of Hungary's National Security Strategy (2012) and the National Military Strategy (2012). According to the latter one, the Hungarian Defence Forces are facing threat not only from the physical dimension but also from the cyberspace. It concludes that "the characteristics of cyber threats which are different from those of conventional threats necessitate a comprehensive review and possible amendment of our concepts of war" (Ministry of Defence 2012, 10/33).

At the organizational level, the highest political coordinating body is the National Cyber Security Coordination Council (supervised by the Ministry of Interior). The body tasked with general cyber-monitoring/capabilities is the National Security Authority (NSA-Hungary). It promotes the protection of classified information and electronic systems handling sensitive data. The Counter Terrorism Centre, established in 2010 within the Ministry of Interior, is the state body expected to deal with cases of disinformation campaigns and cyber-attacks (Janda et al. 2017b). The governmental computer emergency response team (GovCERT-Hungary) is the key unit in charge of identifying cyber incidents (Kovacs and Szentgali 2015). The National Cyber Security Center was established in 2015. The National Electronic Information Security Authority (within the Ministry of Interior) is tasked with assessment and supervision of the data of central and local governmental agencies (Kovacs and Szentgali 2015). The bodies responsible for military cyber monitoring/capabilities are the Computer Incident Response Capability (MilCIRC) and the Military Computer Emergency Response Team (MilCERT). MilCIRC is the umbrella organization above the involved stakeholders in the defence sector. It cooperates with GovCERT-Hungary in handling cyber-security incidents (Kovacs and Szentgali 2015). Intelligence agencies with cyber capabilities are the Constitution Protection Office (internal intelligence) and the Information Office (external

intelligence). Both are involved in non-military intelligence gathering operations. Following a major institutional reorganization, a significant part of Hungary's cyber-defence has fallen under the umbrella of the state intelligence services which affects the transparency of the sector (Visegradinfo 2018). Regarding NATO CCD COE/STRATCOM bodies and activities, the country joined NATO CCD COE in 2010 as a sponsoring nation.

Poland

At the strategic level, there are three key documents which shape the cyber-security framework of Poland: The Cyber Security Strategy of the Republic of Poland for 2016-2020, the Cyberspace Protection Policy of the Republic of Poland (2013) and the Cyber Security Doctrine of the Republic of Poland (2015). Among other priorities set by the National Security Strategy (2014), is to ensure "the security of Poland in cyberspace". The strategy underlines the need for the development of both defensive and offensive capabilities (Swiatkowska, Albrycht, and Skokowski 2017). It also underlines the need to enhance preparedness for any incidence of cyber war and the country's ability to react, either independently or in cooperation with allies (ibid). The recently passed Act on cyber-security (2018) requires key enterprises of the Polish economy to report cyber-incidents to one of existing CSIRT (Computer Security Incident Response Team) (Telecompaper 2018).

At the organizational level, there is no coherent cyber-security system in Poland (Visegradinfo 2018). The main coordinating bodies in the field are the Ministry of Defence and the Ministry of Digital Affairs. While the Ministry of Digital Affairs was without a head for three months in 2018, the Ministry of Defence was put forward as a post of the Governmental Representative for cyber-security was set up there (ibid). The body tasked with civilian cyber-monitoring/ capabilities is the Internal Security Agency aimed to protect the internal security of Polish citizens. The Governmental Computer Security Incident Response Team (CERT.GOV.pl) is in charge of handling cyberspace computer incidents, and emergency responses within the government administration and the civil area (Swiatkowska, Albrycht, and Skokowski 2017). The body tasked with military cyber monitoring/capabilities is the Military Computer Incident Response Team (MIL-CERT PL) at the Ministry of Defence and is concerned with the military cyber-defence. The National Cryptology Centre (supervised by the Ministry) has coordinating tasks in cyber-protection. There are four intelligence agencies with cyber-capabilities, two military and two civilian, each has different cyber-security priorities (ibid). Regarding NATO CCD COE/STRATCOM bodies and activities, two STRATCOM departments operate within the Ministry of Defence and the Ministry of Interior. A new NATO Centre of Excellence for counterintelligence opened in Poland in 2017 (Schindler 2017). Poland is a sponsoring nation in NATO STRATCOM COE and participates in Finnish COE on Countering Hybrid Threats (Janda et. al. 2017).

Slovakia

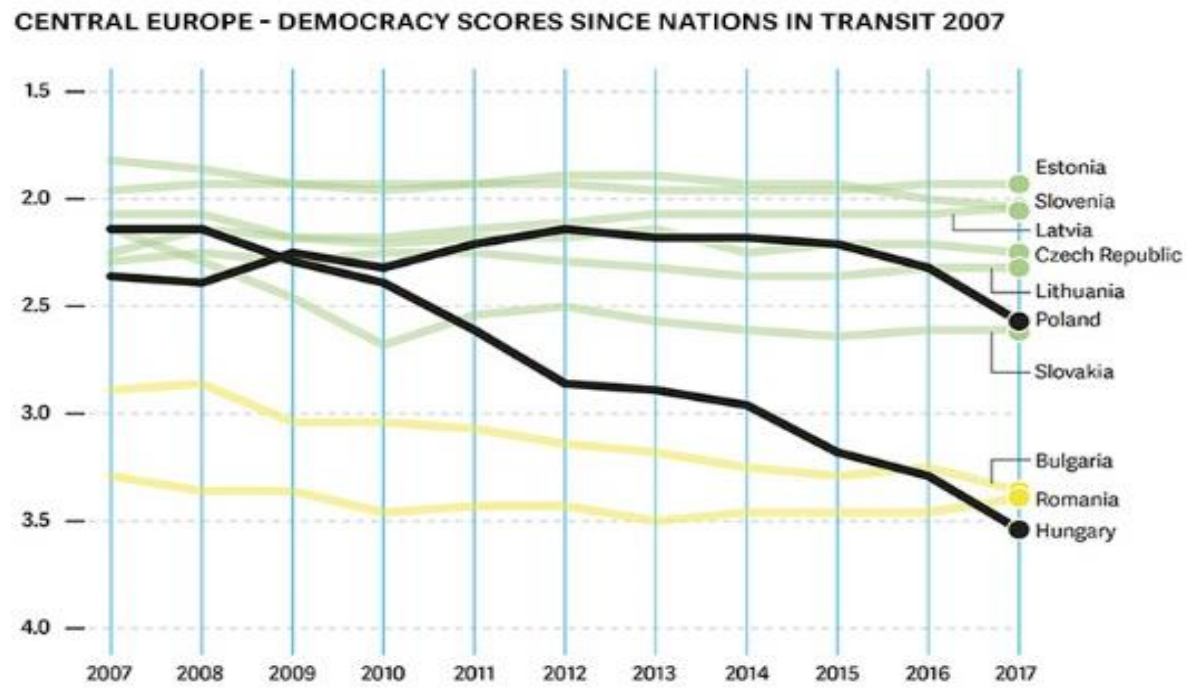
At the strategic level, the National Strategy for Information Security of the Slovak Republic (2009–2013) is the key strategic document behind the Slovak cyber-approach. The strategy was drafted by the Ministry of Finance, the key authority in charge for information security. The three documents that involve tasks concerning the protection of Slovak cyber space are the Cyber Security Concept of the Slovak Republic (2015 – 2020) with the accompanying Action Plan, and the White Paper on Defence of the Slovak Republic. Three of them consider cyber-security a vital component of national security. The Concept recommends four basic mechanisms to be developed: Decision-making and control; Prevention; Reaction; and Restoration mechanisms. The tasks and competencies of the existing cyber-security bodies are defined by the Competence Act and specified by the Cyber Security Act, which came into force (Act No. 69/2018 Coll on cybersecurity).

At the organizational level, the Slovak approach differentiates between the management and information security of classified and unclassified information (Hricikova and Kaska 2015). The main coordinating body is the National Security Authority (NSA-Slovakia), tasked with the protection of domestic cyber-security. The Slovak Computer Emergency Response Team (SK-CERT), provides national and strategic activities in the field of cyber security management, threat analysis, and incident resolution. Cybersecurity Single Information System serves for management, coordination, evidence, and inspection of state administration responsibilities for the area of cybersecurity and CSIRT units. The body tasked with civilian cyber-monitoring/capabilities: The Computer Security Incident Response Team Slovakia (CSIRT.SK) operating under the supervision of the Ministry of Finance ensures the protection of the national information and communication and critical infrastructure. The body tasked with military cyber-monitoring: The Ministry of Defence does not have a direct role in national cyber-security management (Hricikova and Kaska 2015). Nonetheless, the Military Intelligence has specific responsibilities including “detection of state as well as non-state actors’ operations’ in the cyberspace”. The recently established Cyber Defence Center (within the Military Intelligence) has tasks to collect, analyse and evaluate information related to cyber-security and communicate current threats with the affected parties. The Military computer security response team is a part of the Center (CSRT.MIL.SK). The Slovak Information Service that is the leading state intelligence agency also possesses civil cyber-capabilities. It collects technical and open-source intelligence and shares it with other national and international security bodies, such as EU and NATO (ibid). NATO CCD COE/STRATCOM bodies and activities: Slovakia is a part of NATO CCD COE nations. CSIRT.SK took part in Cyber Coalition 2016 and cyber security exercise Cyber Europe 2016. The National Security Authority cooperates with the European Union Agency for Network and Information Security (ENISA) in organizing conferences on the cyber-security (NSA-Slovakia 2018). Slovakia is also among the new members of the Global Index of Cybersecurity NCSI.

Political regime change

Political regimes comprehend the role of information differently – either as a value or means to maintain power. What political regime considers a cyber-threat determines the strategies and policies that governments seek to develop. Security institutions in democratic and non-democratic regimes differ in their functions, responsibilities, and methods of collecting information (Gill, 2007, Scott and Jackson 2010). They also differ in their accountability to society. In democratic states, security organizations are expected to be far more transparent and independent in their actions, whereas, in non-democratic states, such agencies tend to be politically controlled and easily used for political purposes (Bruneau, Dombrovski and Kenneth 2007, Gill 2007). The political shift towards "illiberal democracy" in some of the V4 states makes this discussion particularly relevant. As the concept of "illiberal democracy" seem to be situated within the autocratic-democratic continuum, it is worth analysing how illiberal democracies pursue cyber-security policies. While democratic regimes are more likely to encourage the flow of information through new technologies, autocracies often see this process as an undesirable advantage in the hands of the civil society (Milner 2006). In other words, institutions of autocratic regimes perceive new technologies as a threat to their interest. Consequently, they either restrict new technological development or use it for their own political purposes (Gill 2007).

Graph 1



Source: Freedom House, Nations in Transit 2017.

A 2017 research of the Oxford Internet Institute affirms that the use of social media differs under various political regimes. In authoritarian countries, social media platforms are employed as a key tool of public control (Woolley and Howard 2017). In democracies, social media are actively used for computational propaganda either through opinion manipulation

or targeted experiments on particular segments of the public. For instance, political actors, campaigners, or lobbyists rent broad networks of accounts for campaigning, while governments assign public resources to the creation and use of such accounts (ibid). The same study calls "computational" political propaganda (executed through bots, and algorithm-enhanced human interactions) the most significant threat to democracy (ibid).

Some of the Visegrad states have recently shifted towards illiberal democracies. From a "continuum" perspective, it means that they are neither fully democratic, nor autocratic in relation to information. According to Freedom House's recent report, the average Democracy Score in Central Europe has declined, as "democratic governance in Hungary, a pioneer of "illiberal democracy," has further deteriorated" (Freedom House 2017).

Media freedom in Hungary has experienced significant damages since 2016. Pro-government outlets dominate the media market as government-affiliated owners have purchased national and regional newspapers. The largest independent daily newspaper Népszabadságv closed down in October 2016. Other media platforms and newspapers stopped operating following the 2018 parliamentary election (Magyar Nemzet and Budapest Beacon). In addition, Viktor Orban's government openly targets civil society organizations operating in the country. In May, the Open Society Foundations closed their international operations in Hungary citing increasingly repressive political and legal environment (OSF 2018).

The case of Poland is equally disturbing, according to the same report (Freedom House 2017). The country has demonstrated significant deterioration in the rule of law and adherence to democratic values (ibid). After coming to power in 2015, the right-wing Law and Justice party (PiS) has been systematically undermining institutional checks and balances (The Economist 2017). In 2016, the government took control over the public broadcaster, 164 journalists had resigned or were fired by July 2016 (BBC 2016, The Conversation 2018). According to the coordinator of the Observatory of Media Freedom in Poland Dorota Glowacka, news on public media now can be "manipulative, misleading, or simply untrue" (Koponen and Sanomat 2018). Media experts argue that intentionally misleading stories are not an everyday problem, but they warn that information broadcast on state-controlled media, often not far from propaganda, weakens the overall media environment in the country (ibid).

To sum up, the illiberal democracies born within the Visegrad Four have a rather non-democratic attitude towards the role of information. Some of the states in the region encourage or even actively employ the use of media (including social platforms on the Internet) for political purposes. Therefore, it is difficult to pinpoint what exactly qualifies as "fake news" or a disinformation campaign in those of the Visegrad states where governments are neither supportive towards fundamental values like freedom of speech, nor try to protect them. Illiberal democracies, therefore, are sufficiently conducive to internal and external cyber threats referring to the use of algorithms, automation, and human curation to intentionally disseminate misleading information via social media channels.

The Strategy of Pro-Russian Disinformation Campaigns in the Visegrad states

Disinformation campaigns have recently become a serious threat to the authenticity of the domestic political processes across Europe. Russia is seen as a primary source of disinformation attempts after the annexation of Crimea and the sanctions imposed by the EU in 2014. From a Western point of view, the key strategic goal of Russia is to "successfully create an Eastern Bloc of "Putinverstehers" in the midst of the European Union causing an even greater rift in Trans-Atlantic relations" (Gyori et al. 2017). In 2017, the European People's Party came up with a resolution stating that the "EU Member States are facing an unprecedented threat to their democratic societies. Russian propaganda, disinformation campaigns and continuous support for anti-European political forces are undermining the European project, transatlantic cooperation and Western democracies in general: in terms of liberal values, political independence and sovereignty (EPP Congress 2017)". In 2017 the French and German elections testified to pro-Kremlin efforts to meddle in the domestic politics of a number of European states. Between 2015 and 2017, key intelligence agencies made public statements and issued warnings in relation to Russian interference threats (France, Germany, the Netherlands, the United Kingdom, the Czech Republic, etc.) (Janda et al. 2017a). At least twelve EU member states have updated their policies and enhanced their cyber-security capabilities in light of Russian subversion attempts (Gyori et al. 2017).

Table 2: Common characteristics of pro-Kremlin propaganda in the Czech Republic and Slovakia:

Heavily use conspiracy theories, and combine facts and half-truths
Strongly anti-Western, most frequently targeting the United States, Ukraine, and West in general
To a lesser extent Pro-Kremlin and pro-Putin
Claim no allegiance to Kremlin
Send and use very similar messaging and arguments
Have negative undertones, usually depicting moral, economic, political and social degradation and predicting a bleak future of collapse and civilization clashes
Frequently using loaded language and emotionally charged words, stories, and pictures
Are interconnected and supported by various public personalities that give campaign both credibility and public visibility

Source: Smolenova 2015

Visegrad states have been among the targets of extensive pro-Russian propaganda following the annexation of Crimea in 2014, various strategic updates, research documents, and media reports show. Russian influence across the region comes via various channels including

economic, political and disinformation actors. Though all Visegrad states have had predominantly negative historical experience with Russia, political and economic links have been lately rationalized by domestic power circles (Gyori et al. 2017). On one hand, the communist past of the region allows for rediscovering of preexisting political and economic links to Moscow. On the other hand, Russia openly favors politicians in each of the Visegrad countries.

Disinformation campaigns largely facilitate the impact of pro-Kremlin political and economic actors at the local level and successfully channel Russian interests in the region. A massive number of media outlets, webpages, fake Facebook and Twitter accounts have generated content and influenced online discussions in favour of Moscow's political agenda.

Another report on Russian influence in Central and Eastern Europe indicates that Moscow is behind a decentralized system of webpages and social network accounts operating locally (Gyori et al. 2017). This disinformation "octopus" has been in charge for the production of anti-globalist and anti-Western narratives retransmitted by pro-Russian far-right parties, paramilitary organizations and representatives of Russian intelligence services active in the region (Snyder 2018, Polyakova and Boyer 2018, Gyori et al. 2017, Shekhovtsov 2017).

A recent study by *European Values* overviews the EU states' responses to pro-Kremlin subversion operations (Janda et al. 2017b). The authors look at 1) Political acknowledgement of the threat; 2) Government Counter-activities, and 3) Counter-intelligence activities. The research shows that some Visegrad states are more concerned with pro-Russian activities than others (see Table 1). While Hungary and Slovakia are "ignorant" in their countermeasures, the Czech Republic and Poland are in the group of "the cognizant" (ibid). Hungary and Slovakia belong to the group of countries who largely ignore or deny the existence of Russian disinformation operations. On the contrary, the Czech Republic and Poland have experienced a strategic shift of "awakening" after the annexation of Crimea and, therefore, are determined to fight external political interference (ibid). The report illustrates a wide gap between the acknowledgement of the threat and concrete counter-measures developed at the state level.

According to the GLOBSEC Vulnerability Index, Hungary is the most vulnerable country in the Visegrad group to subversive Russian influence, followed by Slovakia (Milo and Klingova 2017). The two states are weakest, as they use relations with Moscow for domestic political purposes. The Czech Republic occupies the third place among the Visegrad Four. Poland is the least vulnerable to hostile foreign operations, the Index shows (ibid). The country has consistently expressed concerns about Russia's foreign policy behavior. Thus, Poland and the Czech Republic appear to be more active in dealing with the disinformation threats than Hungary and Slovakia.

*Table 3: Overall ranking of the countermeasures undertaken by the V4 states to the Russian subversion operations (*Political engagement in cyber-security 5=Strongest, 0=Weakest)[3]

Group	Country	Political acknowledgement of the threat	Government Counter-activities	Counter-intelligence activities	Total
Ignorant	Hungary	1	0	1	2
	Slovakia	1	1	1	3
Cognizant	Czech Republic	4	3	4	11
	Poland	4	3	5	12

Source: "Overview of countermeasures by the EU28 to the Kremlin's subversion operations", European Values 2017

This policy brief argues that Visegrad states' responses to pro-Kremlin propaganda differ depending on each country's relationship with Russia. Disinformation attempts are not equally seen as a security issue by the national governments in the Czech Republic, Hungary, Slovakia, and Poland although they represent a specific form of a cyber-threat. While some of the governments in the region securitize them through political statements and strategic documents, others offer an environment conducive to foreign "fake news" attacks by simply not acknowledging their harm to the political process. Moscow's meddling in recent election campaigns[4] has been rather welcomed, even openly endorsed by some local pro-Kremlin political actors (Gyori et al. 2017).

Government Perceptions and Response

Czech Republic

Historically, the Czech society has been sensitive to pro-Russian influence due to its Soviet-era legacy (BIS 2017). Politically, the country has openly expressed its security concerns about the Kremlin's actions in relation to the annexation of Crimea. Since 2014, the Czech online space has been under attack by pro-Russian propaganda. In 2016, Russian hackers carried out "very active" cyber-attacks against several Czech institutions (Chamonikolas 2017). The Russian hacking group APT targeted diplomatic, military and academic bodies in the same year when the Czech legislative election took place (ibid). By using IP addresses outside the country, the hackers successfully corrupted private emails of people affiliated with the military (ibid). The same group is known to be linked to cyber-attacks against the Democratic Party in the U.S., the White House, and NATO. According to the Czech security

[3] The table operationalizes the scale for each of the three measures. The bigger/smaller numbers mean a stronger/weaker political engagement with the cyber-security.
[4] The Czech legislative election, 2016, Austrian legislative election, 2017 and the Hungarian parliamentary election in 2018.

service (BIS), the cyber espionage is a part of increased activities of Russian intelligence agents in the country (ibid). In its 2017 annual report, the Czech Military intelligence (VZ) informs about an increase in cyber espionage aimed at collecting classified data on the defence of the Czech state in 2016.

Though Prague is generally concerned with cyber-threats posed by Russia, key political actors, like the president Milos Zeman, undermine the strategic resistance at the state level. Re-elected in 2018, Zeman has lobbied for lifting the sanctions against Russia, repeatedly denied the presence of Russian troops in Eastern Ukraine and called for the recognition of Crimea as part of Russia (MacFarquhar 2016). He also maintains strong ties to Russian business circles (Milo and Klingova 2017). A report by European Values (2018) shows the role of disinformation campaign in the 2018 presidential election when Milos Zeman's key opponent Jiri Drahos became a target of a massive disinformation campaign on social media. He was portrayed as a former collaborator of the Czech secret police from the communist times, a supporter of unrestricted immigration, and even a paedophile (Krejci, Vichova, and Janda 2018). These false reports appeared on propaganda outlets, social media pages and e-mails. Drahos lost by less than 3% of the votes as one of the contributing factors, according to the report, was exactly the extensive disinformation campaign launched against him (ibid).

The response: As it was noted, there is a clear shift in the strategic documents of the Czech Republic, following the annexation of Crimea (Kremlin Watch Team 2017a). The Concept of the Czech Republic's Foreign Policy (2015) states that "Russia currently severely destabilizes the European security architecture" and that "Czech policy towards Russia will depend on the respect of the Russian Federation for international law and for the territorial integrity and sovereignty of its neighbours" (Ministry of Foreign Affairs 2016). In the 2015 Security Strategy of the Czech Republic, Russia is not directly mentioned by name, but it is clear that main security concerns are linked to its actions. Furthermore, the Czech Security Strategy is very specific when describing trends of hybrid threats (Article 19). It mentions the threat of other powers to build a sphere of influence through a combination of political, economic and military pressure (Elemir Necej and Samuel Zilincik 2017). The Czech Defence Strategy (2017) notes that Russia uses a set of hybrid campaign tools against members of NATO and the EU, including targeted disinformation activities and cyber-attacks (Ministry of Defence of the Czech Republic 2017). In the long run, the Czech Ministry of Defence is concerned with the growing misuse of information, technologies, and media for information warfare at the international level (Ministry of Defence of the Czech Republic 2015). The National Security Audit (2016) has identified various types of hybrid threats, among them terrorism and foreign disinformation campaigns (Kremlin Watch Team 2017a). It contains two chapters specifically concerned with cyber hazards: Influence of Foreign Powers and Hybrid Threats (ibid).

At the operational level, the establishment of the Centre against Terrorism and Hybrid Threats is the specific response to disinformation campaigns. An inter-agency working group was established to protect the 2016 elections, as the existing cyber-security institutions

offered briefings on this matter for political actors who competed in the parliamentary vote (Janda et al. 2017a). Furthermore, the Czech intelligence has been very concrete in its assessment of the disinformation attacks coming from Moscow. They list the specific aims of Russian information operations in the Czech Republic in 2015, including weakening the Czech media through massive production of Russian propaganda and disinformation; strengthening the information resistance of the Russian audience, exerting influence on the perceptions and thoughts of the Czech audience, weakening public's will for resistance through relativization of truth and objectivity (promoting the motto "everyone is lying"), creating or promoting inter-societal and inter-political tensions in the Czech Republic through foundation of puppet organizations, covert and open support of populist or extremist subjects, etc. (Kremlin Watch Team 2017a).

Hungary

Today's government in Budapest is rather often on the same page with Moscow on key issues like migration, human rights or national security, despite the negative historical experience with Russia. Following the annexation of Crimea, the Hungarian PM Viktor Orban (re-elected in 2018 for a third consecutive term) tries to weaken the EU sanctions against Russia calling them a mistake (BBC 2014). He has been strengthening the political and economic relationship with Russia to levels not seen after the democratic transition in Hungary (Kreko 2017). Orban's meetings with Vladimir Putin are the most frequent, compared to other EU leaders. On one hand, Hungarian PM employs its "friendship" with Russia for domestic political and economic purposes. Good relations between Budapest and Moscow fuel and are fuelled by authoritarian policies. Russia officially and unofficially endorses Orban's agenda targeting foreign NGOs, opposition, media, minority and migration groups. Russia is also a crucial economic, trade, and energy partner for Hungary (Janda et al. 2017).On the other hand, the "friendship" with Russia serves as a tool in his anti-EU rhetoric, as Moscow tends to encourage Eurosceptic and autocratic elements across Europe (Janda et al. 2017a, Conley et al. 2016). In addition, the far-right opposition party *Jobbik* openly promotes the Kremlin's interests at the domestic level, "reportedly receiving Russian financial support" (Conley et al. 2016).

The response: There is reluctance in Hungary to admit Russian influence. Disaffirmation campaigns seem to be part of the political mainstream, efficiently disseminated via pro-government media outlets. A 2017 Freedom House report notes that in some cases, the Hungarian government is more inclined to enable the spread of Russian influence and conduct disinformation campaigns (Freedom House 2017). A large segment of the Hungarian mainstream media is under the control of the government, as some outlets systematically use Russian state media like Sputnik or RT as primary sources in their own coverage (ibid). A recent analysis by Political Capital shows how pieces of disinformation have been circulating in politically-controlled media outlets. The article looks at five examples, including the 2014 Maidan revolution in Ukraine, the disappearance of the Malaysia Airlines flight 370, the assassination of the Russian opposition leader Boris

Nemtsov, the 2016 Brussels terror attack and the Panama Papers scandal (Hungarian Spectrum 2018).

The official strategic and security documents of Hungary do not consider Russian cyber behaviour a threat. The National Security Strategy broadly acknowledges that the state will meet "increasingly pressing and intricate challenges in the physical and virtual space of information technologies and the potential malicious use of these technologies by state and non-state actors" (Janda et al. 2017). The Counter Terrorism Centre established in 2010 within the Ministry of Interior is the state body expected to deal with cases of disinformation campaigns and cyber-attacks (Janda et al. 2017b). However, disinformation campaigns have not been considered a serious issue by the government. As NGOs and civil groups are under a systematic attack by the government, they are highly limited in their attempts to raise awareness or investigate disinformation campaigns.

Poland

Poland is among the most concerned EU member states about the Russian foreign-policy activities. Historically, the Soviet invasion of Poland in 1939 and the Katyn Massacre in 1940 left deep scars in the political relationship between the two countries. There are also recent reasons for deepening the gap between the two states, namely the Smolensk plane crash in 2010, where the former Polish President Lech Kaczynski and other state officials lost their lives (Janda et al. 2017a). The country has security concerns due to a shared border with the Kaliningrad Oblast. Following the annexation of Crimea, Poland has fully supported the EU sanctions against Russia.

In the aftermath of the Ukrainian crisis, the Polish Facebook space and news portals were flooded with a large number of pro-Kremlin fake accounts intervening in the discussions related to Russia and Ukraine (Gorwa 2017, Savytsky 2016). In 2015, the Polish Computer Emergency Response Team expresses a great concern about Russian influence in the cyberspace of Poland, and especially via social networks (CERT Poland 2015, Gorwa 2017). There was an active targeting of online forums and Facebook groups attacked touching upon the Russian-Ukrainian conflict. They were attacked with spam comment sections and hostile posts (ibid). A recent report has argued that a variety of dubious outlets spread false information in an attempt to undermine the NATO Summit held in Warsaw in 2016 (Wierzejski, 2016). From fabricated interviews with high-ranking Polish military leaders to sensational attempts to stir up Polish-Ukrainian tensions, the report cites multiple cases in which anonymous "journalists" and bloggers, believed to be linked to Russia, published dubious information that was spread on social media (ibid). Meanwhile, civic groups and activists were threatened on Facebook when they dared to engage in discussions on Russian-Ukrainian-Polish relations. Previous research has identified that a very small number of suspected bot accounts are responsible for a large proportion of activities on related political hashtags. A recent study indicates that a small number of hyperactive right-wing accounts

generate more than 20% of the total volume of political Twitter activity over a three-week period (Gorwa 2017).

The response: According to the annual address of the minister of foreign affairs, from 2016 Poland recognizes Russia as a threat at a political level stating that the Kremlin seeks influence Eastern European countries by using means of hybrid activities, including propaganda: "Our policy towards the Russian Federation is unfortunately determined by Russia's aggressive actions in Eastern Europe" (Ministry of Foreign Affairs 2017). In 2015, Poland requested the enhanced presence of NATO and also expanded its military budget from 1.6% GDP in 2013 to 2.2% in 2015 (ibid). Although Russia is not specifically described as a threat in any strategic and security documents, there are four key factors, according to the Polish Security Strategy, determining security in Europe: NATO, EU, the strategic presence of the US on the European continent and relations with Russia (Art. 34). Article 41 assesses Russia's position as follows: "Russia's relations with the West will remain an important factor influencing the security of Poland, the region, and Europe. The attempt to restore Russia's status as a major power at the expense of its neighbourhood, as well as the escalation of its confrontational policy, exemplified by the conflict with Ukraine, including the accession of the Crimea, has a negative impact on security in the region" (NSS 2014, 21/41).

According to a 2014 report of the Internal Security Agency, there is a high level of activity of the Russian intelligence services in Poland appearing in the form of a broad spy network (Janda et al. 2017a, Schindler 2017). The aim of the Russian influence operations, the same report says, was to discredit the position of Poland and other NATO member states in the Ukraine crisis, to bring attention to the complex history of relations between Poland and Ukraine in order to cause antagonism between their societies, and to create and divisions among EU and NATO members (ibid). According to the report, there is an attempt by the Russian side to spread pro-Russian and anti-Ukrainian views among the Polish public through internet blogs, portals, and news services. The documents describe the activities of paid internet trolls as well as so-called 'useful idiots' (ibid).

Slovakia

The Slovak cyberspace has been highly conducive to pro-Russian disinformation campaigns in the recent years. Like in the other Visegrad states, websites generating pro-Kremlin propaganda have been particularly active following the conflict in Ukraine and later the refugee crisis. The extreme far-right magazine Zem a Vek and the state media outlet TASR have announced a "content sharing with Sputnik (Tamkin 2017, Benkova 2018). Like other Visegrad states, Slovakia had negative political experience with Russia in the past. The country has supported the EU measures against Russia following the annexation of Crimea. However, due to energy dependence and economic ties with Russia, "in gestures and declarations, Slovakia remains one of the most pro-Russian countries in the EU" (Kalan and Vass 2015). Pro-Kremlin local political successfully maintain Russian interest in the country

(Conley et al. 2016). Russia's intervention in Ukraine has played a serious role in raising the Slovak authorities' interest in building up national cyber-security capacities, according to Maros Kirnak, the director of the Cyber Security Programme at the Slovak Security Policy Institute (Adamowski 2017).

The response: The government in Bratislava does not consider Russian influence a threat, therefore, does not securitize disinformation campaigns and does not give a priority to strategic counter-measures (Milo and Klingova 2017). The opportunistic attitudes of the Slovak political elite towards EU and NATO and President's energy ties to Russia (Kremlin Watch 2017) largely affect the general state resilience to Russia's influence in the form of disinformation campaigns. Slovak political elite is not concerned with Russian propaganda, with the exception of the President Andrej Kiska (Janda et al. 2017a). In 2015, during a meeting with the NATO General Secretary Jens Stoltenberg, he warned against the danger of disinformation campaigns. In March 2017, he publicly stated that "Slovakia is a target of information war and propaganda and Slovak security services are doing next to nothing to counter it" (17th Annual Foreign Policy Review Conference, 2017).

Foreign propaganda is mentioned in the 2015 annual report of the Slovak Military Intelligence Services but does not name specific actors perpetrating these activities (Janda et al. 2017a). Article 9 of the current National Security Strategy lists four features of the current security environment: 1) Promotion of foreign-political interests by some states and their use of military force to disrupt the territorial integrity of other; 2) Increase in the occurrence of terrorist attacks; 3) Violation of international law; and 4) the Increase in the number of failed states in the EU's neighbouring regions. The first and third points are related to the policy of Russia, although it is not explicitly mentioned (Necej and Zilincik 2017). In addition, Article 18 of the draft points to the negative impact of hybrid activities that both state and non-state actors can use to achieve specific goals without a formal declaration of war (ibid). The document describes the Slovak approach towards Russia as a pragmatic one, with emphasis on economic and cultural cooperation. Comparing to the Czech and the Polish security strategies, the Slovak one is generally less critical towards the Kremlin (ibid). The country does not actively participate in efforts to counter disinformation at the international level (Janda et al. 2017a).

Unlike the political elite, civil society in Slovakia is a strong player in countering disinformation campaigns. Few research organizations try to address the issue, among them the Slovak Forum against Propaganda, The Slovak Security Policy Institute and the Globsec Policy Institute (Janda et al. 2017a). The initiative Konspiratori.sk is aimed at countering pro-Kremlin disinformation attacks. Activists like Juraj Smatana also contribute to the reaction. He has collected data on more than 100 disinformation websites active in Slovakia and Czech Republic (Smolenova 2015).

Conclusion

All four, the Czech Republic, Hungary, Poland, and Slovakia have been targets of pro-Russian disinformation campaigns in the recent years. Channels that distribute misleading information have emerged in the "national" cyber-space of all the Visegrad states. Nonetheless, not all of them see the phenomenon as a security problem. Generally, it is a challenge to define disinformation campaigns, especially in those of the Visegrad states where media freedom is damaged due to state capture and the introduction of "illiberal" practices. Hungary and Slovakia, more receptive to pro-Russian political agendas, are less active in countering "fake news", attempts for manipulating online discussions and more generally subversive activities in the cyberspace. As both, external and internal (governmental) propaganda "speak" the same language on certain issues, Russian disinformation campaigns cannot be easily identified and addressed adequately. The lack of active political resistance against pro-Russian local actors undermines the possibility for a comprehensive reaction at the state level. Furthermore, the lack of strong democratic institutions in some of the countries does not allow for tackling disinformation campaigns effectively and prevent the democratic process from large-scale damages.

All the Visegrad states differ in how they define and address cyber-security threats, and more specifically, disinformation campaigns. They rely on different institutional and technical capacities, experience political regime changes and also develop distinct relationships with Russia. In all four states, cyber- security management is rather state-centralized, while horizontal engagement with private stakeholders, research centres, and civic groups remain underdeveloped. Although the EU-level adopted documents allow for a greater cooperation among the V4 states in fighting disinformation campaigns, such efforts might be seriously challenged by domestic political affairs. Unless the countries overcome these differences, we can hardly expect a common approach to cyber-security in the region that will pave the way for the V4 to more comprehensive regional and international initiatives with a focus on disinformation campaigns.

This policy paper was published by STRATPOL

Responsible editor: Ondřej Zacha

STRATPOL – Strategic Policy Institute
office@stratpol.sk
+421 908 893 424

www.stratpol.sk

References

Act No. 181 of 23 July 2014 On Cyber Security and Change of Related Acts (Act on Cyber Security) https://www.govcert.cz/en/legislation/legislation/

BBC. 2014."Hungary PM Orban condemns EU sanctions on Russia". August 15, 2014. Accessed June 29, 2018. https://www.bbc.co.uk/news/world-europe-28801353.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. University of Munich, published in association with Theory, Culture & Society.

Benkova, Livia. 2018. "The Rise of Russian Disinformation*".* Austrian Institute for European and Security Policy. Accessed August 4, 2018. https://www.aies.at/download/2018/AIES-Fokus-2018-03.pdf.

Botond, Feledy. 2017. *Parallel Competences: The State of Cyber Security in V4.* Visegrad Insight. November 30, 2017. Accessed April 27, 2018. http://visegradinsight.eu/parallel-competences-the-state-of-cyber-security-in-the-v4/.

Bruneau, Thomas C. and Dombroski, Kenneth R.2014. Reforming Intelligence: The Challenge of Control in New Democracies. Naval Postgraduate School.

Chen, Adrian. 2015. *The Agency*. The New York Times. June 2, 2015. Accessed July 25 2018. https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Conley, Heather A, James Mina, Ruslan Stefanov, and Martin Vladimirov. 2016. *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe.* Center for Strategic & International Studies. Accessed April 27, 2018. http://public.eblib.com/choice/publicfullrecord.aspx?p=4714770.

CSIRT.SK is the governmental/national CSIRT (Computer Security Incident Response Team), accessed August 8, 2018. https://www.csirt.gov.sk/.

CERT Polska, The Governmental Computer Security Incident Response Team (CERT.GOV.PL), accessed 8 August, 2018. https://www.cert.pl/en/.

Daniel Milo, and Katarina Klingova. 2017. *Vulnerability Index: Subversive Russian Influence in Central Europe.* Accessed May 2, 2018. GLOBSEC Policy Institute. https://www.globsec.org/wp-content/uploads/2017/08/globsec-vulnerability-index.pdf.

European People's Party. Russian disinformation undermining Western democracy. Resolution. EPP Congress, Malta, March 2017. Accessed August 4, 2018. https://www.epp.eu/files/uploads/2017/04/6-EPP-Resolution-1.pdf.

Estonian Presidency of the Council of the European Union. 2017. Tallinn Digital Summit conclusions published: creating a digital continent. Press Release. Oct 6, 2017. Accessed June 23, 2018. https://www.eu2017.ee/news/press-releases/tallinn-digital-summit-conclusions-published-creating-digital-continent

Gallacher, John, et. al. 2017. "Social Media and News Sources during the 2017 UK General Election". *The Computational Propaganda Project.* Oxford Internet Institute. Accessed May 2, 2018. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Social-Media-and-News-Sources-during-the-2017-UK-General-Election.pdf.

Gill, Peter. 2007. *Handbook if Intelligence studies*. Routledge.

Gill, Peter and Mark Phythian. 2001. *Intelligence Theory: Key Questions and Debates.* Routledge.

Gorwa, Robert. 2017.*"Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere".* University of Oxford. Working Paper No. 2017.4

Government Incident Response Team – Hungary. Accessed 8 August 2018. http://www.cert-hungary.hu/en/node/6.

Gyori, Lorant, Peter Kreko, Jakub Janda, and Bernhard Weidiner. 2017. *Does Russia Interfere in Central Europe's Elections.* Political Capital, European Values Think-tank in cooperation with DöW. Accessed April 28, 2018. http://www.politicalcapital.hu/pc admin/source/documents/western_experiences_eastern_vulnerabilities_20171012.pdf

Forelle, Michelle and Phil Howard, Andres Monroy-Hernández, and Saiph Savage. 2015. *Political Bots and the Manipulation of Public Opinion in Venezuela.* Accessed May 7, 2018. http://arxiv.org/abs/1507.07109

Freedom House. 2017. Freedom of Press 2017. Hungary. Accessed May 2, 2018. https://freedomhouse.org/report/freedom-press/2017/hungary.

Freedom House. 2017. *Nations in Transit 2017.* Accessed May 4, 2018. https://freedomhouse.org/report/nations-transit/nations-transit-2017.

Hansen, Lene and Nissenbaum, Helen. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly*. Vol. 53. Issue 4. 1155–1175. Accessed April 28, 2018. https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf.

Hare, Forrest. 2010. "The cyber threat to national security: why can't we agree". CCD, COE Publications, Tallinn, Estonia. Accessed April 27, 2018. https://ccdcoe.org/sites/default/files/multimedia/pdf/Hare%20-%20The%20Cyber%20Threat%20to%20National%20Security%20Why%20Cant%20We%20Agree.pdf

Hardt Michael and Negri Anconio. 2004. *Multitude: War and Democracy in the Age of Empire.* New York. Penguin Books.

Holcova, Pavla et. al.2017. "Propaganda targets Czechs, Slovaks and Hungarians differently". Spectator. 27 November, 2017. Accessed August 4. 2018. https://spectator.sme.sk/c/20704641/propaganda-targets-czechs-slovaks-and-hungarians-differently.html.

Hungarian Spectrum. 2018. "Russian Disinformation in the pro-government Hungarian media", accessed July 29, 2018. http://hungarianspectrum.org/2016/08/27/russian-disinformation-in-the-pro-government-hungarian-media/.

Janda, Jakub, et. al. 2017a. *Overview of Countermeasures by the EU28 to the Kremlin's Subversion Operations.* European Values. http://www.europeanvalues.net/wp-content/uploads/2017/05/Overview-of-countermeasures-by-the-EU28-to-the-Kremlin%E2%80%99s-subversion-operations-1.pdf

Janda, Jakub, et. al. 2017b. *How Do European Democracies React to Russian Aggression.* Accessed April 29, 2018. http://www.evropskehodnoty.cz/wp-content/uploads/2017/04/How-do-European-democracies-react-to-Russian-aggression-1.pdf

Kalan, Dariusz, and Agnes Vass. 2015. *Big Gestures, Small Actions: Paradoxes of Slovakia's Policy towards Russia.* The Polish Institute of International Affairs. No. 43 (775). Accessed May 10, 2018. https://www.pism.pl/publications/bulletin-no-43-775.

Koponen Henri Mikael and Sanomat Helsingin. 2018 "Poland's division hinders fight against "fake news". International Press Institute. Accessed July 25, 2018. https://ipi.media/polands-division-hinders-fight-against-fake-news/.

Krejčí, Markéta, Veronika Víchová, and Jakub Janda. 2018. *The Role of the Kremlin's Influence and Disinformation in the Czech Presidential Elections.* European Values, Kremlin Watch Report. Accessed April 29, 2018. http://www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-Czech-presidential-elections.pdf.

Kreko, Peter. 2017. *Hungary: Crackdown on Civil Society à La Russe Continues.* May 18, 2017. Accessed May 1, 2018. https://www.csis.org/blogs/international-consortium-closing-civic-space/hungary-crackdown-civil-society-%C3%A0-la-russe.

Kremlin Watch Team. 2017a. *Policy Shift Overview: How the Czech Republic Became One of the European Leaders in Countering Russian Disinformation.* European Values. Accessed April 26, 2018. http://www.europeanvalues.net/wp-content/uploads/2017/05/Policy-shift-overview-How-the-Czech-Republic-became-one-of-the-European-leaders-in-countering-Russian-disinformation-1.pdf.

Kremlin Watch Team. 2017b. *Kremlin Influence in Visegrad Countries and Romania: Overview of the threat, Existing Countermeasures, and Recommended next steps.* European Values. Oct 23, 2017. Accessed April 27, 2018. http://www.europeanvalues.net/wp-content/uploads/2017/12/Kremlin-Influence-in-Visegrad-Countries-and-Romania.pdf

Krystof, Chamonikolas. 2017. "Czech Republic Says Russian Hackers Were "Very Active" There in 2016" Bloomberg. Accessed June 24, 2018. https://www.bloomberg.com/news/articles/2017-10-24/russian-fancy-bear-hackers-seen-very-active-in-prague-in-2016.

Laszlo Kovacs, and Gergely Szentgali. 2015. *National Cyber Security Organization: Hungary.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). https://ccdcoe.org/multimedia/national-cyber-security-organisation-hungary.html.

Lea Hricikova, and Kadri Kaska. 2015. *National Cyber Security Organization: Slovakia.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). Accessed May 5, 2018. https://ccdcoe.org/multimedia/national-cyber-security-organisation-slovakia.html.

MacFarquhar, Neil. 2016. "How Russians Pay to Play in Other Countries." The New York Times, December 30, 2016, Accessed May 8, 2018. https://www.nytimes.com/2016/12/30/world/europe/czech-republic-russia-milos-zeman.html.

Maurer, Tim. 2018. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

Minarik Tomas. 2016. *National Cyber Security Organization: Czech Republic.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). Accessed May 5, 2018. https://ccdcoe.org/multimedia/national-cyber-security-organisation-czech-republic.html.

Ministry of Defence. 2012. Hungary's National Military Strategy. Accessed May 4, 2018. http://2010-2014.kormany.hu/download/b/ae/e0000/national_military_strategy.pdf.

Ministry of Defence of the Czech Republic. 2015. The Long Term Perspective for Defence 2030. Accessed May 4, 2018. http://www.army.cz/images/id_8001_9000/8503/THE_LONG_TERM_PERSPECTIVE_FOR_DEFENCE_2030.pdf

Ministry of Defence of the Czech Republic. 2017. Defence Strategy of the Czech Republic. Accessed May 4, 2018. http://www.army.cz/assets/en/ministry-of-defence/strategy-and-doctrine/defencestrategy2017.pdf.

Ministry of Foreign Affairs of the Republic of Poland. 2016. Annual Address: Information of the Minister of Foreign Affairs on Polish Foreign Policy Tasks in 2017. Accessed May 2, 2018. http://www.msz.gov.pl/en/foreign_policy/goals_of_foreign_policy/annual_address_2011/.

Ministry of Foreign Affairs of the Czech Republic. 2015. Concept of the Czech Republic's Foreign Policy. March 8, 2015. Accessed May 4. 2018. https://www.mzv.cz/jnp/en/foreign_relations/policy_planning/concept_of_the_czech_republic_s_foreign.html

Ministry of Defence of the Slovak Republic, accessed 8 August, 2018. http://vs.mosr.sk/o-nas/eng.

Milner, Helen V. 2006. "The Digital Divide – The role of political institutions in Technology Diffusion." *Comparative Political Studies*, Vol 39, No 2, p 176 – 199. http://journals.sagepub.com/doi/10.1177/0010414005282983.

National Security Bureau of the Republic of Poland. 2014. National Security Strategy of the Republic of Poland. Accessed May 4, 2018. https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf.

NATO News. 2015. "NATO and Czech Republic Bolster Cyber Defence Cooperation. October 12 2015. Accessed 14 May, 2018. https://www.nato.int/cps/en/natohq/news_123857.htm.

National Cyber and Information Security Agency (NUKIB). 2014. Act on Cyber Security and Change of Related Acts (Act No. 181/2014 Coll.). Accessed May 5, 2018. https://www.nbu.cz/cs/pravni-predpisy/1091-zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/.

National Security Authority of the Slovak Republic, accessed 8 August 2018. http://www.nbusr.sk/en/index.html.

National Cyber and Information Security Agency https://www.govcert.cz/en/.

Scmagazineuk. 2017. Czechs build new cyber-security HQ. Adamowski, Jaroslaw, 3 January 2017. Accessed 8 August, 2018. https://www.scmagazineuk.com/czechs-build-new-cyber-security-hq/article/1475590.

Necej, Elemir, and Samuel Zilincik. 2017. *Analysis of the Draft of Security Strategy of Slovak Republic 2017: Comparison with Strategic Documents of Czech Republic and Poland.* Stratpol. Accessed May 8, 2018. http://stratpol.sk/analysis-of-the-draft-of-security-strategy-of-slovak-republic-2017-comparison-with-strategic-documents-of-czech-republic-and-poland/.

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security". *Ethics and Information Technology.* June 2005, Vol. 7, Issue 2, 61-73. Accessed April 26, 2018. https://www.nyu.edu/projects/nissenbaum/papers/ETINsecurity.pdf.

Official Journal of the European Union. 2016. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Accessed May 5, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

Official Journal of the European Union. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016. Accessed May 5, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

Official Journal of the European Union. 2008. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The Council of the European Union. 23 Dec 2008. Accessed May 5, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114.

Open Society Foundation. 2018. "The Open Society Foundations to Close International Operations in Budapest". Accessed June 21, 2018. https://www.opensocietyfoundations.org/press-releases/open-society-foundations-close-international-operations-budapest.

Polyakova, Alina and Spencer P. Boyer. 2018. The Future of Political Warfare: Russia, the West, and the coming year of global digital competition. Brookings – Robert Bosch Foundation Transatlantic Initiative. Accessed July 25, 2018. https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf.

PragueMonitor. 2017. Military intelligence: Cyber spying becomes more frequent. 25 Oct 2017. Accessed 8 August, 2018. http://www.praguemonitor.com/2017/10/25/military-intelligence-cyber-spying-becomes-more-frequent.

Savytskyi, Yuriy. 2016. Kremlin trolls are engaged in massive anti-Ukrainian propaganda in Poland. *Euromaidan Press.* June 20, 2016. Accessed July 26. 2018. http://euromaidanpress.com/2016/06/21/kremlin-trolls-are-engaged-in-massive-anti-ukrainian-propaganda-in-poland/

Schindler, John. 2017. "Poland Pushes Back Against Putin's Special War". Observer. Oct 10, 2017. Accessed June 29, 2018. http://observer.com/2017/10/poland-pushes-back-against-putins-special-war/.

Scott, Len and Peter Jackson. 2010. "The Study of Intelligence in Theory and Practice". *Intelligence and National Security*. 139-169. Vol 19.2004. Issue 2.

Security Information Service (BIS) – Intelligence Service of the Czech Republic. Accessed May 13, 2018. https://www.bis.cz/defaultEN.html.

Shekhovtsov, Anton. 2017. *Russia and the Western Far Right: Tango Noir*. Routledge.

Swiatkowska, Joanna, Izabela Albrycht, and Dominik Skokowski. 2017. *National Cyber Security Organization: POLAND.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). Accessed May 1, 2018. https://ccdcoe.org/multimedia/national-cyber-security-organisation-poland.html.

Telecompaper. 2018. "Polish President signs cyber-security act" 7 August 2018. https://www.telecompaper.com/news/polish-president-signs-cyber-security-act--1255864

The Slovak Republic reached the top place in the global index of cybersecurity NCSI. NSA http://www.nbusr.sk/news/the-slovak-republic-reached-the-top-place-in-the-global-index-of-cybersecurity-ncsi/index.html.

Tamkin, Emily. 2017. "The Real Russian Threat to Central Eastern Europe". Foreign Policy. March 30, 2017. Accessed August 4, 2018. https://foreignpolicy.com/2017/03/30/the-real-russian-threat-to-central-eastern-europe-2/

Woolley, Samuel C., and Philip N. Howard. 2017. "Computational Propaganda Worldwide: Executive Summary". *Working Paper No. 2017.11.* Oxford University Press. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Visegradinfo. 2018. "Is Visegrad group ready for cyber-attacks?" By: Zachova, Aneta and Edit Zgut, Karolina Zbytniewska and Lucia Yar. 2018. May 7, 2018. Accessed July 26, 2018. http://visegradinfo.eu/index.php/80-articles/560-is-visegrad-group-ready-for-cyberattack