Defending critical communication infrastructures against bot and troll armies in Central-Eastern Europe

Policy Recommendations
27 March 2020

POLITICAL CAPITAL
POLICY RESEARCH & CONSULTING INSTITUTE

British Embassy Budapest

Introduction

The defence of critical communication infrastructure has become a major issue for most of the countries in Central-Eastern Europe, as well as in the West faced with the Kremlin's repeated attempts to influence public attitudes on the war in Ukraine or elections in France, Germany, the UK or the United States. The COVID-19 epidemic has also proven that Russian or Chinese actors, including state officials, used the health emergency to extend their soft or sharp power by spreading false information about the virus to sow discord and panic in Ukraine or among Western nations, members of the European Union or NATO[1].

Therefore, with the generous support of the British Embassy in Budapest, Political Capital organised an online conference on 25 March 2020 addressing the "Defense of critical communication infrastructures against bot and troll armies in Central-Eastern Europe". Renowned experts such as **David Patrikarakos**, the author of War in 140 Characters, or **Wojciech Przybylski**, the editor-in-chief of Visegrad Insight explored how state or non-state actors, market-based solutions could enhance NATO's and Central-European countries' resilience to disinformation disseminated by domestic actors or foreign autocracies. Expert discussions were distilled to produce a set of policy recommendations detailed in this paper to increase Central-European states' and societies' capability to fight disinformation in times of crisis, such as the COVID-19 epidemic.

Research data further revealed that the problem of mass-manipulation attempts utilising troll, bot or hybrid armies does not only concern foreign autocratic powers and their influence in our region,[2] but populist governments who are also keen on spreading domestic propaganda and disinformation for electoral purposes, as it has been happening, for example, in Hungary. Moreover, the problem presents itself even on a more general level, since almost all democratic governments have engaged in disinformation activities in varying degrees, while Western societies have proven to be a breeding

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap

ground for cutting-edge manipulation technologies and platforms as part of strong and advanced democratic and economic competition, according to the Oxford Internet Institute.[3] A case in point is Facebook, which has not only provided billions of people and millions of civic organisations with tools to present and publish themselves to the local or global audiences but became a powerful tool of political manipulation harvesting the personal data of millions of American voters as well, which became known as the Cambridge Analytica scandal.[4]

The stakes are high both domestically and regionally or globally. Whereas Central-European countries' economic prosperity depends on the EU and their national security on NATO, as Wojciech Przybylski wrote in his article in Visegrad Insight,[5] disinformation driven by anti-elitist conspiracy theories weakens public trust and support for NATO, the EU or the Transatlantic community. Based on Globsec Trends 2019,[6] more than a third of Central-Europeans would support a European army as an alternative to NATO, while more than half of respondents distrust mainstream media and consume content on fringe sites spreading disinformation on a regular basis. The role of Russian disinformation in the growing disorientation of Central-European or Western societies about their own political or military establishments cannot be overestimated. Political Capital's research on the projection of Russian "sharp power"[7] utilising both negative or positive messaging to manipulate foreign audiences along the Kremlin's various foreign policy goals has shown that Russia is perceived as "bigger or better" when it comes to military or hybrid capabilities by over a third of the populations in the Czech Republic, Slovakia and Hungary.

Thus, the definition and defence of critical communication infrastructure boil down to desired or undesired geopolitical scenarios or futures for the CEE region and the Euro-Atlantic community. If democracies are successful in reigning in the influence of foreign autocratic powers and disruptive technological platforms used for spreading disinformation, they can achieve economic and political prosperity and improve the global competitiveness of Western security and political integration against a rising China or a militarily active Russia. Were these infrastructures overwhelmed by crises and related mass manipulation attacks, we are not only faced with the possible disintegration of Euro-Atlantic security structures and establishments, Central-Eastern European countries will inevitably need to deal with Russian or Chinese attempts to exert not only soft, sharp or economic power, but political or digital hegemony over the region.[8]

The definition of critical communication infrastructure

1. **Critical infrastructure can be defined as those assets that are essential for the functioning of a society, economy and the political system.** Therefore, the definition of critical infrastructure cannot be limited to governmental institutions or properties, and it needs to encompass all kinds of civilian or non-civilian sectors ranging from nuclear reactors to financial or market communication services.[9]

2. Consequently, **the defence of critical infrastructures** against malign foreign influences, including troll and botnet activities **needs to address all the online or offline vulnerabilities of the critical sectors** that can be targeted by online mass-manipulation attacks or campaigns.

3. State or non-state actors need to cooperate to identify those sensitive, cutting-edge technological sectors that are underregulated or developing so fast that the protection of users, companies and state-actors is lagging behind adversaries' manipulation capabilities.

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap

Recommendations related to the COVID-19 crisis

1. **The crisis related to the COVID-19 epidemic has created multiple power "vacuums" for adversaries.** One geopolitical vacuum allows Russia or China to proactively influence NATO member states' domestic narratives through disinformation in their favour, while there is a lack of strategic communication on the part of the Euro-Atlantic Community or the EU to counter such mass-manipulation attacks. A marketing "vacuum" related to deteriorating financing and investment into mainstream media makes the production of disinformation and related cybercrimes, frauds "cheaper" for domestic or foreign malign actors. As Miroslava Sawiris from Globsec Policy Institute put it during the conference:

   "The Slovak information space has been flooded with a lot of positive articles about how China is dealing with the whole epidemic, how Russia is helping. Their message has been very vicious against the EU, how the EU is failing. (…) If we look at how much effort the Kremlin's administration actual invests into sending out their messages, I am not sure our state- or EU-level (investments) can even be compared compete. (…) It is about more investment into strategic communication and being aware of the fact that it is crucial, it is not some kind of add-on service."

2. **The current crisis proves that adequate preparations would be needed on the state level to establish specialised agencies capable of dealing with crisis communication and foreign disinformation** taking advantages of crises. European and Central-European countries should follow the lead of the Czech Republic, which successfully debunked misleading Chinese narratives about the epidemic through the Centre Against Terrorism and Hybrid Threats established under the Ministry of Interior in 2017. David Stulík's view, who is a Senior Analyst of the Kremlin Watch Program at European Values Center for Security Policy, is that:

   "The narrative says (…) 'the totalitarian regimes are able to cope with the disease, the pandemic more efficiently than democratic societies', (…) 'we the Chinese are helping you a lot'. In the Czech Republic, the government sent aid to China, and within one month, we were basically buying the same protective things from China overpriced. It is showing this kind of a cynical tonality of the Chinese narrative. (…)

   In the Czech Republic, it turned out, it was kind of a wise decision a few years ago to establish the Center against Terrorism and Hybrid threats (…), because these people there have structures, have communication channels that were immediately used as the crisis was unfolding. They were very effective in fighting health-related disinformation. (…) The second institutional body, which turned out to be a very right decision to establish, was the National Agency for Cyber Protection, because (…) there were hacker attacks on one of the two hospitals that were established to cure and treat people with COVID-19. (…) We had these specialists (…) who immediately assisted this hospital."

3. **In times of crisis, such as the current COVID-19 epidemic, state and non-state actors need to formulate an effective "biopolicy" considering both the vulnerabilities of the healthcare system and foreign or domestic online manipulation events**, such as health-related disinformation, conspiracy theories, external active measures that are designed to cripple the effective use of the health services or undermine public trust in the public emergency management establishment in a given country.

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap

Countering disinformation in the CEE

1. **Members of the Transatlantic community could aid local societies and governments in formulating a standard strategic communication strategy against Russian or Chinese propaganda** attacks rooted in the regional drivers of disinformation of "insecurity" about geopolitical belonging between the East and the West, and the sense of historical "inferiority" to big powers.[10]

2. Governments would need to coordinate more on a regional or European level to adopt each other's best institutional approaches, best state or non-state practices fending off foreign authoritarian influences coming from Russia or China.

3. State and non-state defence capabilities against mass-manipulation attacks would need to be assessed and utilised separately, as individual government's willingness to produce domestic propaganda or disinformation might hamper local civil society actors' efforts to counter disinformation effectively.

4. Mass-manipulation attacks against CEE political establishments and NATO infrastructure would need to be addressed differently since Central-European societies' trust, or distrust in international organisations varies significantly. Thus, for example, Czech responses countering disinformation would focus more on Euroscepticism, while the Slovak response would need to deal more with the anti-NATO sentiment of its citizens, while Polish society's positive view on the United States would render any foreign-born disinformation attack against NATO less effective.

5. **The apolitical youth in the CEE region**, which mostly consumes political news via friends and social media platforms, **would need to be educated through special online courses** on how to identify and fight politically motivated disinformation using a mixture of political or apolitical, and lifestyle-related communication.

6. The high level of distrust towards traditional media combined with the frequent consumption of content on pro-Kremlin or fringe disinformation sites in the region would require Central-European governments to support the freedom of media, freedom of speech, and the plurality of media, The aim of these efforts would be to enhance public resilience against troll or botnet attacks, and disinformation with the help of trusted international or local media.

7. **Local state and non-state actors would need to join their effort to achieve some form of data or "information sovereignty"** in cooperation with Western media platform providers, such as Google, Facebook or Microsoft, against autocratic foreign adversaries well-versed in online manipulation techniques and attacks.

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap

Recommendations regarding NATO's cyber policy strategy

1. **Partners should further develop their capacities to respond to below-the-threshold attacks**. Moreover, they should agree on the goal and means of systematic responses to malicious cyber activity that would fall below the threshold of armed conflict.

2. **Further development of the principle of 'imposing a cost on those who harm us' is necessary**. Intertwining with the previous point, below-the-threshold attacks should not be left unanswered and the response should be deteriorating, while of course, respecting international law.

3. **Pro-active approach, political will and serious commitment is needed from the allies on self-defence in the cyber domain as well**. As we witness tendencies showing cyber threats to have a more and more severe impact, partners should address the challenges associated with operating in the cyberspace. Hence, partners should consider taking further steps anticipating further means and ends regarding cyber warfare.

4. Allies will have to harmonise and reconsider how to respond both individually and as an alliance to respond to attacks below the threshold of armed conflict. They should make use of Article 4 of the Washington Treaty.

5. The problem of attributability of below-the-threshold attacks should be readdressed: while absolute certainty is required for legal action, less is enough for some other responses.

6. Allies might want to adjust their priorities and resourcing to a certain degree. As the authors of a recent study point out,[11] the Cyber Operations Center (CyOC) is considered to have a key role in adapting NATO Command Structure for the cyberspace, as we can expect it to develop further once the initial capacities, resources and the sufficient number of specially educated experts are available. Therefore, NATO needs to address the question of recruiting and retaining personnel in the long run, focusing on attracting talent and expertise.

7. Besides defensive capabilities, offensive capabilities should be developed as well in cyberspace. Many experts find the current situation parallelled to the 1950s when the superpowers were experiencing a sudden void, with new technologies and no set rules. Hence they mutually tried to deter the other by demonstrating military capabilities. Knowing that they can mutually destroy each other demotivated them to use their weapons to more than just deterrence. As by then, pre-emptively demonstrating cyber warfare capabilities now might be key to guarantee long-lasting peace, not only to react to possible attacks.

   As Krisztián Jójárt, an external fellow at the National University of Public Service, Centre for Strategic and Defence Studies said:

   "At the moment, what is going on is the strategic signalling of capabilities".

   Péter Krekó, Director of Political Capital said:

   „The function of trolls and bots is that they create a false illusion of mass support behind some sometimes very marginal opinion. If you do that, you mislead the audience, and I think it is a real, moral question of how far the West can go. And you can not necessarily fight fire with fire all the time. So, I think this reactive approach is morally justifiable, and I think we could see it in many cases (…) that even the officially most prepared and most developed countries can meet these challenges totally unprepared. And I think that's why we have to analyse, track and show to the public instances of authoritarian exploitation of the cyber domain; they need to see responses."

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap

8. **NATO's strategic communication should become more effective in crises, such as the COVID-19 epidemic**. While adversaries, like China or Russia, used the current crisis to take advantage of the Western political responses and the establishment's disorientation to catapult their disinformation narratives into the media spaces of member states, the alliance seems quite inefficient in this regard.

9. Not only NATO as a whole should communicate more effectively, but its sub-divisions as well, especially in the cyber domain: while there are centres of excellence such as StratCom in Riga, its existence is not known among the wider public. Average citizens should be made aware of its existence and of the fact that contrary to what they might think, NATO is present, capable and actively working on their protection. As Wojciech Przybylski, the editor-in-chief of Visegrad Insight put it:

   "We had NATO troops in Italy opening field hospitals (…) before the Chinese involvement of selling masks, not delivering aid – it went under the radar."

Recommendations regarding the market and civil society solutions

1. **Market or civic actors could act as intermediaries between citizens and state institutions**, bureaucracies in channelling resources from institutional levels to individuals, harnessing scattered societal innovations in all walks of life for public use by public institutions.

2. **Social media and online platform providers should adopt self-regulative measures** to protect their sectors from mass-scale abuses and use their cutting-edge technologies, novel services to defend individual and state actors against foreign information attacks.

3. **Market actors' increasingly AI-driven services could be trained to defend against the infiltration of online communities** aimed at societal polarisation, the flooding of online platforms or communities with disinformation, and supporting societal resilience to disinformation by directing grassroots communication to original, non-manipulated contents.

4. **Countries' response to disinformation should rely on "information sovereignty" that combines market-solutions with regulatory approaches in order to provide national security based on a healthy information environment, capable of withstanding foreign autocratic power projections in the information space.** This kind of sovereignty should address both the adequate financing of mainstream media capable of producing fact-based, objective reporting and the fight against digital fraud preventing investments into digital markets. In Wojciech Przybylski's view:

   "It is a prerequisite of a democracy to have a certain level of information sovereignty, but not as it is defined by the Chinese or Russians in the sense of control over it. Democratic actors should rather provide society with all the tools necessary for critical reception and understanding (news), and the ability to distinguish fake from real."

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap

Notes

1 'Russia Deploying Coronavirus Disinformation to Sow Panic in West, EU Document Says', Reuters, 18 March 2020, https://www.reuters.com/article/us-health-coronavirus-disinformation-idUSKBN21518F.

2 The NATO Strategic Communications Centre of Excellence distinguishes between "classic trolls" who "act in their own interests solely with the aim of sowing disagreement and inciting conflict in the online environment" and "hybrid trolls" who "are employed as a tool of information warfare" by state-actors. See: https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

3 'Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation – The Computational Propaganda Project', accessed 23 March 2020, https://comprop.oii.ox.ac.uk/research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/.

4 Alex Hern, 'How to Check Whether Facebook Shared Your Data with Cambridge Analytica', The Guardian, 10 April 2018, sec. Technology, https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica.

5 'The Real Tragedy of Central Europe - Visegrad Insight', accessed 23 March 2020, https://visegradinsight.eu/the-real-tragedy-of-central-europe-illiberalism/.

6 'GLOBSEC Trends 2019: Central and Eastern Europe 30 Years after the Fall of the Iron Curtain', GLOBSEC (blog), accessed 23 March 2020, https://www.globsec.org/publications/globsec-trends-2019/.

7 Lóránt Győri, 'Larger than Life - Who Is Afraid of the Big Bad Russia? Grassroots Vulnerability to Russian Sharp Power in Hungary Country Report' (Political Capital, May 2019), https://politicalcapital.hu/pc-admin/source/documents/pc_larger_than_life_hungary_eng_web_20190514.pdf.

8 'Eastern European Futures - Visegrad Insight', accessed 23 March 2020, https://visegradinsight.eu/eap2030/.

9 'Critical Infrastructure Sectors | CISA', accessed 23 March 2020, https://www.cisa.gov/critical-infrastructure-sectors.

10 Lóránt Győri and Péter Krekó, 'Larger than Life - Who Is Afraid of the Big Bad Russia?' (Political Capital, April 2019), https://www.politicalcapital.hu/pc-admin/source/documents/pc_larger_than_life_eng_web_20190410.pdf.

11 Ablon, Lillian, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, and Julia A. Thompson, Operationalizing Cyberspace as a Military Domain: Lessons for NATO. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/perspectives/PE329.html.

Political Capital Policy Research and Consulting Institute
H-1037 Budapest, Montevideo street 2/c, 2nd stairwell, 2nd floor
Phone: +36 1 430 66 99
www.politicalcapital.hu
Email: info@politicalcapital.hu
https://twitter.com/Pol_Cap