COI HYBRID INFLUENCE

Hybrid CoE Paper 6

APRIL 2021

Deterring disinformation? Lessons from Lithuania's countermeasures since 2014

VYTAUTAS KERŠANSKAS

Hybrid CoE Paper 6

Deterring disinformation? Lessons from Lithuania's countermeasures since 2014

VYTAUTAS KERŠANSKAS

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They can be either conceptual analyses or be based on a concrete case study with empirical data.

The COI Hybrid Influence looks at how state and non-state actors conduct influence activities targeted at Participating States and institutions, as part of a hybrid campaign, and how hostile state actors use their influence tools in manners that attempt to sow instability or curtail the sovereignty of other nations and independence of institutions. The focus is on the behaviours, activities, and tools that a hostile actor can use. The goal is to equip practitioners with the tools they need to respond to and deter hybrid threats. The COI HI is led by the UK.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253 800 www.hybridcoe.fi

ISBN (web) 978-952-7282-70-0
ISBN (print) 978-952-7282-71-7
ISSN 2670-2053

April 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

Contents

1. Introduction[1]

Russia's aggression against Ukraine in 2014 was the most virulent materialization of its revisionism of the post-Cold War European security architecture. The information domain was also targeted. Indeed, the volume of war propaganda and disinformation designed to shape the international community's perceptions of the conflict more favourably towards Moscow was unprecedented. This was a red flag for the Euro-Atlantic community – free speech and the media, key pillars of democracy, were being weaponized to an extent unseen in decades.

The same conclusion was drawn in Lithuania. Even though Russian disinformation had already been identified as a challenge, it only became widely recognized as a pressing national security threat in 2014. An immediate response ensued, and countering disinformation became a key priority in dealing with hybrid threats. This mobilized not only the government, but also civil society and the private sector. Although the main actor in countering disinformation was the government, the latter two also played an important supportive role in enabling a robust response to an acute challenge.

In the first part of this article, a brief description of the Lithuanian information environment, and the context and objectives of the Russian disinformation against/in Lithuania is provided. The main actions taken by the government, civil society and the private sector to counter the threat since 2014 are presented in the second part. An assessment of the impact of both – disinformation and countermeasures – is discussed in the third part. The article concludes with some key lessons learnt and recommendations for policymakers.

Even though Lithuania did not have a 'deterrence strategy' for dealing with disinformation, the analysis of the countermeasures taken provides valuable insights into the application of deterrence principles to non-military threats. To this end, this article attempts to challenge the notion that disinformation cannot be deterred. The analysis shows that countermeasures were divided between denial (including resilience-building) and the imposition of costs, and that such an approach helped to decrease the spread, severity, and impact of Russian disinformation.

Consequently, this case study supports the contemporary approach to the deterrence of emerging security threats, such as hybrid threats, which suggests that deterrence strategies should aim at fully dissuading hostile actors from conducting intolerable malign activities, while simultaneously mitigating low-level hostilities by denying their negative effect.

1 Vytautas Keršanskas is a Defence Policy Group Advisor at the Ministry of National Defence of the Republic of Lithuania. The ideas presented in this article are exclusively his own and should not be considered an official position of the Ministry or its departments.

2. Russian disinformation in Lithuania: Context and objectives

Disinformation is contextual, so describing the historic, sociological, and other important factors is crucial before explaining why particular measures were taken in Lithuania to counter this threat.

The Soviet occupation (1940–1941 and 1944–1990) experienced by the Lithuanians is inevitably an important factor. The Soviet regime could not survive without its huge security apparatus or strong and widespread propaganda, which was employed over all areas of life. Some who believed unconditionally in 'the Soviet story' were taken in, although the narrative was also rejected by many who were able to identify the propagandistic messages. Reading 'between the official lines' was a competence many people developed during the era.

Consequently, the majority of those living in the newly independent Lithuania in the 1990s had vivid memories of the Soviet propaganda. After 30 years of independence, Lithuanians who can still recall this era are in the 50+ age group. Some continue to believe in 'the Soviet story'. According to polls, approximately 20 per cent of the population still believe that life was better under Soviet rule, and the percentage is higher among older age groups.[2] On the other hand, the majority of the population is rather dismissive, or at least less susceptible to information originating from the Kremlin.

This is not to say that they are immune – disinformation has become more sophisticated through the use of narratives that correspond to the current thinking and beliefs of the targeted groups.[3] But the vivid memory of Soviet propaganda is a factor that makes it easier to explain the threat of weaponized information to that part of society which is identifiable as a vulnerable group.

For example, Kremlin propaganda about the Maidan revolution being 'fascist' was naturally rejected by the majority in Lithuania, including the older generation, because such narratives were constructed following the same patterns as those used by the Soviets against the National Independence movement in Lithuania when it was still occupied. Therefore, this vivid memory, coupled with widespread solidarity with the historically related Ukrainian nation among Lithuanians, mobilized society and made recognition of the severity of the disinformation threat much easier.

A second important factor concerns the information consumption habits in Lithuania. Television remains the main information source: a 2020 survey suggested that 66 per cent of the population watch TV daily, while an additional 13 per cent watch it two to three times a week.[4] Five per cent of respondents reported that they watched Russian TV daily, and another six per cent claimed to watch it two to three times a week. A 2016 survey conducted among Lithuanian Russians and Poles suggested a sharp contrast to the general population: 57 per cent of Russians and 42 per cent of Poles said that they watched Russian television on a daily basis, while 26 per cent of Russians and 23 per cent of Poles said that they watched it several times a week.[5]

Even though the Lithuanian Russian minority is much smaller compared to the other Baltic states (around 6 per cent in Lithuania compared to

2 Linas Kojala (ed.), *Geopolitikos ir tarptautinės politikos bei grėsmių suvokimo tyrimas* [*Research on the Perception of Geopolitics, International Politics and Threats*], (Rytų Europos studijų centras, 2020), 25-26, https://www.eesc.lt/wp-content/uploads/2020/07/RESC-tyrimas.pdf. Last accessed 19 April 2021.
3 Andrius Vaišnys et al., *Rusijos propaganda: analizė, įvertinimas, rekomendacijos* [*Russian propaganda: Analysis, Evaluation, Recommendations*] (Rytų Europos studijų centras, 2017), 155, http://www.eesc.lt/uploads/news/id987/RESC%20monografija_propaganda.pdf. Last accessed 19 April 2021.
4 Kojala (ed.), *Geopolitikos ir tarptautinės politikos bei grėsmių suvokimo tyrimas*, 46-48.
5 Vaišnys et al., *Rusijos propaganda: analizė, įvertinimas, rekomendacijos*, 155.

around 25 per cent in Latvia and Estonia), it is still quite a sizeable target audience. As suggested, the Polish minority (around 6 per cent of the population) fall under the same target group, due to historical consequences and their media consumption habits.

Knowledge of foreign languages is an important factor here. Six out of ten Lithuanians know Russian,[6] and for the 50+ age group it is frequently the only foreign language they know. This is the reason why information influencing happens not only in the form of disinformation campaigns, but also by employing 'soft power' means, such as subsidized TV broadcasts of Russian origin.

Other factors that make particular societal groups potential targets are their economic situation, education, level of trust in the media or government, or – in a broader sense – their geopolitical preferences and emotional attachment to statehood.[7] The global trend of the growing popularity of social media as the main news source for younger citizens is also visible in Lithuania, which is an additional element in an already complex environment.

A third important point is related to the core Russian disinformation principle of targeting different audiences with specific narratives that appeal to each one in particular. Such a targeted approach boosts the effectiveness of disinformation and enables multiple goals to be achieved by a singular campaign. In the Lithuanian case, the main audiences are the national minorities, disappointed patriots, citizens with conservative moral values, or those who do not have a strong opinion on issues related to geopolitics or international politics.[8]

Four main objectives of Russian disinformation in Lithuania could be identified:[9]

1. To create tensions between different groups in Lithuanian society (primarily the Lithuanian majority and national minorities).
2. To damage Lithuania's image among its allies and partners and vice versa (mainly by exploiting and manipulating cleavages between different interpretations of history, but also more bluntly through fake news stories).
3. To enhance support for Russia's policies (either by promoting Russia's approach or by discrediting the West).
4. To create a wedge between the state and its citizens (with the aim of decreasing the will to resist, trust in political institutions, etc.).

The unprecedented level of war propaganda and disinformation spread by Russia in 2014, the identified objectives listed above, and the recognized vulnerabilities led to a situation whereby Russian disinformation was immediately seen as a 'hard security' threat. Such conclusions were simultaneously drawn by politicians, media representatives and civil society alike – the key stakeholders in responding to such a threat. As a result, 2014 became a turning point whereby countering disinformation came to be a systemic and strategic objective with all of the key stakeholders involved.

6 Lietuvos statistikos departamentas, 'Gyventojai pagal išsilavinimą ir kalbų mokėjimą' [Population by education and language skills], https://osp.stat.gov.lt/informaciniai-pranesimai?eventId=1699. Last accessed 19 April 2021.
7 Ibid., 76-78.
8 Diana Janušauskienė et al., *Ar Lietuvos gyventojai jaučiasi saugūs? Subjektyvus saugumas kintančiame geopolitiniame kontekste* [Do Lithuanian citizens feel safe? Subjective security in the changing geopolitical context] (Vilnius: Lietuvos socialinių tyrimų centras, 2017), 80.
9 Lietuvos Respublikos valstybės saugumo departamentas, 'Grėsmių nacionaliniam saugumui vertinimas' [*Assessment of the national threats by the State Security Department*] (2014), 9, https://www.vsd.lt/wp-content/uploads/2016/10/Gresmiu-vertinimas-2014.pdf. Last accessed 20 April 2021.

3. A swift response in 2014: Measures to counter disinformation

After the Russian disinformation threat was identified as a pressing security challenge in 2014, immediate actions were taken to achieve a two-fold objective – **to reduce the amount of Russian disinformation and to neutralize its negative impact as quickly as possible.** The immediate reaction was similar to the way in which other democratic nations had responded, mainly by boosting media monitoring and strategic communication capabilities, and undertaking media literacy and awareness- raising initiatives to increase societal resilience.

Yet it was quickly recognized that resilience-building is a long-term endeavour, and that other measures that have an immediate effect must be combined. An existing legal framework allowed the Radio and Television Commission of Lithuania to temporarily suspend the broadcasts of the Kremlin-controlled TV channels. This was duly applied, serving to both deny access to hostile information and impose costs for inappropriate behaviour. Implemented in an early phase, it also signalled resolve.

In the initial years when the Russian disinformation flow was extremely high, short-term mitigation was prioritized. This led to a large number of governmental and non-governmental initiatives to raise societal awareness of the disinformation threat or to impose costs (mainly by suspending Russian TV channel broadcasts) as a response to the most harmful disinformation campaigns. But longer-term initiatives were undertaken simultaneously to gradually boost societal and institutional resilience, to build an institutional arrangement for quick and effective mitigation of disinformation campaigns, to review the legal basis, and to develop targeted measures that could deal with the identified vulnerable elements (e.g. national minorities, regional media and similar).

The two tables presented below capture the most significant measures or actions taken between 2014 and 2020 by the Lithuanian government, civil society or private sector to counter Russian disinformation, and the main reasoning behind each action. The actions are not listed in any specific order. Moreover, in order to provide insights for the discussion on the application of deterrence to hybrid threats, a short note on the relevance of each activity to the deterrence principles for dealing with hybrid threats[10] is included.

Table 1 lists the measures or actions taken by the Lithuanian government, its institutions, or officials (politicians). These measures mainly fall into three categories: regulating the information space, making strategic communications effective, and using international leverages. These measures were implemented to reduce the amount of Russian disinformation and to neutralize its negative impact as quickly as possible, as well as to raise the international community's awareness of the Russian disinformation threat.

Table 2 lists the initiatives that were implemented by civil society or the private/non-governmental sector. Some of the initiatives were partly funded by the government, especially those related to resilience building and academic research. However, all of them were grassroots measures advanced by civil society and/or the private sector, and they were well received and encouraged by the authorities because they were seen as providing solid support in achieving a common goal. Close collaboration between governmental and non-governmental representatives was strong from the beginning, which also indicated

10 See Vytautas Kersanskas, *Deterrence: Proposing a more strategic approach to countering hybrid threats*, Hybrid CoE Paper 2, March 2020, https://www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence.pdf. Last accessed 19 April 2021.

TABLE 1. Governmental actions responding to Russian disinformation since 2014

Action or measure	Key objective (why the measure was adopted)	Relevance to the deterrence principles
Russian TV broadcast suspension or ban	• To use existing legal/regulatory instruments as a response to unacceptable activities. • To narrow the direct access to the target groups.	Imposes costs, denies access to a targeted audience.
Tightening media rules and regulations	• To de-incentivize the broadcasting of Russian content, which is seen as a 'soft power' tool. • To narrow the direct access to the target groups. • To change information consumption habits in the long term.	Denies access and benefits.
Boosting information space/media monitoring	• To increase the capacity of the government for early warning, trend analysis, and attribution, which enables both counter-response and long-term planning.	Creates agility, better situational awareness and swifter response. Increases the technical capacity to attribute malign campaigns to the actors behind them.
Establishment or empowerment of the strategic communication bodies in key institutions (MFA StratCom, Government Office)	• To move from responsive to proactive mode in shaping the narrative (both nationally and internationally). • To build working relationship between the governmental institutions and media that could be used to swiftly counter foreign disinformation campaigns.	Promotes agility, swifter response with bigger impact.
Creation of a mechanism for strategic communication coordination on national security matters	• To increase information sharing. • To integrate strategic communication across government on national security matters (speak with 'one voice'). • To have a unified disinformation threat assessment criterion.	Creates a shared understanding of the baseline threat landscape in the information domain across government.
International partnerships and initiatives, using multilateral institutions	• To boost information sharing and coordinate response. • To show resolve (in the form of high-level initiatives or statements). • To review and strengthen international (European) regulation to make counter-disinformation more effective.	Creates solidarity: more efficiency in resilience building, denial of perceived benefits and imposition of costs for unacceptable behaviour.

TABLE 2. Non-governmental initiatives responding to Russian disinformation since 2014

Action or measure	Key objectives	Relevance to the deterrence principles
Civil campaign 'Lithuanian elves' – active citizens fighting disinformation online	• To track the trends of disinformation techniques on social media and the internet, and to exchange information. • To use existing measures on social media to disable disinformation channels (groups, bots, etc.).	Grassroots support for the government enables a whole-of-society response. Both denies access/ benefits and imposes costs.
Debunk.eu – an AI-driven platform for media monitoring	• To use new technologies (AI) to track disinformation. • To raise societal awareness and have a trusted platform for fake news debunking.	Media-driven initiative enables private-public partnership for better situational awareness and more efficient communication.
Increased academic research and public surveys	• To provide evidence-based analysis for informed decision-making and strategic planning.	
Media literacy projects dedicated to vulnerable groups (national minorities, elderly, youth)	• To increase media literacy among various (targeted) groups.	Supports resilience building (denial of benefits).
Social media campaigns – various initiatives created to pursue one's own narrative	• To rid the Lithuanian social media space of disinformation enablers (especially active in the initial years). • To show the determination of civil society to respond to foreign adversarial activities with initiatives such as a boycott of Russian-produced goods, and boosting one's own narrative on topics manipulated by Russia etc.	Supports resilience building (denial of benefits). Signals society's resolve to respond to unacceptable adversarial behaviour.
Media projects for fact-checking and debunking	• To increase societal awareness via fact-checking, debunking and other means.	Supports resilience building (denial of benefits).

the overall resolve and sent a powerful signal to the disinformation spinners in the Kremlin. These activities made the response to Russian disinformation more comprehensive.

In summarizing the activities of the government, civil society and the private sector, there is one important aspect worth mentioning. Resilience-building measures are usually at the core of any debates on countering disinformation, but when it comes to an actual response, a much wider spectrum of tools and measures were employed in the Lithuanian case. It was already recognized in an early phase of the response that an immediate effect requires measures to be taken that either deny benefits, or impose costs for inappropriate behaviour.

Over time, the counter-disinformation strategy crystallized, and involved elements of both resilience and deterrence. Societal resilience was seen as an important enabler for the government to react more swiftly and strongly (e.g. to impose costs by suspending TV broadcasts), but it also enabled a whole-of-society response. Institutional resilience mainly denied the benefits – better and more capable governmental bodies, and established information exchange channels between government communicators and the media neutralized multiple disinformation campaigns at a very early stage.

4. Measuring the impact

One of the key challenges in countering disinformation concerns measuring the impact. This applies to both the impact on the targeted audiences of disinformation campaigns, and the effectiveness of the countermeasures to mitigate the threat. In this section, several examples of different indicators used in Lithuania are presented.

For the most part, the analytics used to measure the severity of a disinformation campaign are quantitative, namely analyzing the spread of the fake message in the traditional, online or social media, and the audience response (most easily measured in social media through shares, likes, retweets, etc.) However, such analytics do not tell the whole story, and more qualitative analysis is required to identify the overall effect of long-lasting disinformation efforts, and to gain a better sense of the effectiveness of the counter-actions.

In 2017, a team of researchers published a study in which key Russian disinformation narratives were identified and a sociological survey conducted.[11] The results were subsequently analyzed to gain insights into the extent to which Russian narratives are supported in society; to understand which information sources are consumed and how they correlate to the first point; and to identify the most vulnerable groups that are more susceptible to disinformation. The results of the study informed decision-makers and helped them allocate resources in a more targeted way.

Public opinion polls (societal 'temperature-taking') are now conducted annually, helping to identify trends in societal perceptions, media consumption and other aspects that assist decision-makers in adjusting their counter-disinformation activities.

In the case of Lithuania, the annual surveys show rather positive trends, for example: a constantly decreasing number of respondents who believe that 'life was better under Soviet rule', increasing support for the Lithuanian military, and no visible changes in society's geopolitical perceptions – continuous support for belonging to the West.[12] Together with other identified indicators, the data collected in the surveys is instrumental when adjusting the implemented activities. Another study published yearly analyzes how much Russian-originating content appears on the main Lithuanian TV channels. Given that television remains the main information source for some societal groups, this 'soft power' tool is important in the long-term objectives of Russian disinformation. The analysis suggested that the number of Russian broadcasts on Lithuanian television increased alarmingly between 2007 and 2017: if there were 79 hours of such broadcasts per week in 2007, the figure doubled in 2016, and peaked in 2017 with 198 hours in total.[13] In response, a law was passed requiring 90 per cent of TV broadcasts to be in Lithuanian or another official EU language. Coupled with some other adjustments, this has resulted in a constant decrease in Russian broadcasts for the past couple of years.[14]

An indicator worth mentioning is the amount of advertising revenue generated by Russian-owned media broadcasting in Lithuania. In 2014, when overall awareness of the disinformation threat spiked, there was a sharp decrease in revenue

11 Vaišnys et al., *Rusijos propaganda: analizė, įvertinimas, rekomendacijos*, 155.
12 Kojala (ed.), *Geopolitikos ir tarptautinės politikos bei grėsmių suvokimo tyrimas*.
13 Vaidas Saldžiūnas, 'Lietuvos televizijų tyrimas: rusiška produkcija minta du kanalai' [Lithuanian TV study: Russian broadcasts feed two channels], Delfi, 17 March 2017, https://www.delfi.lt/news/daily/medijos-karas-propaganda/lietuvos-televiziju-tyrimas-rusiska-produkcija-minta-du-kanalai.d?id=74073260. Last accessed 19 April 2021.
14 Darius Tarasevičius, 'Televizijų transliacijose mažėja rusiškos produkcijos' [Number of Russian TV broadcasts decreases], Verslo žinios, 30 June 2019, https://www.vz.lt/rinkodara/medijos/2019/06/30/televiziju-transliacijose-mazeja-rusiskos-produkcijos. Last accessed 19 April 2021.

for the most popular Russian TV channels "NTV Mir Lietuva" and "RTR Planeta".[15] The decrease occurred as a result of several decisions by the Radio and Television Commission of Lithuania to temporarily suspend the broadcasts of these and other Russian TV stations, as investigations concluded that the content being broadcast violated Lithuanian law.[16] Social pressure – growing negative attitudes towards businesses that advertised on disinformation channels – also played an important role.

These indicators need to be analyzed together, and the regular assessments are really helping policy-planners to come up with the most cost-effective counter-disinformation strategy.

15 BNS, 'Lietuvoje mažėja rusiškų televizijos kanalų reklamos apimtys' [Advertising volumes on Russian TV channels decrease in Lithuania], Delfi, 16 September 2014, https://m.diena.lt/naujienos/verslas/ekonomika/lietuvoje-mazeja-rusisku-televizijos-kanalu-reklamos-apimtys-649205. Last accessed 19 April 2021.

16 Investigations into multiple cases concluded that the Russian TV broadcasts violated the European Union Audiovisual Media Services Directive and the Republic of Lithuania Law on the Provision of Information to the Public because the content repeatedly incited hatred among nations and instigated war.

5. Conclusions and recommendations

The measures taken by the Lithuanian authorities and supported by various initiatives taken by the media, NGOs and civil society have yielded considerable results. Firstly, measures employed to build resilience and to deny the perceived benefits narrowed the possibility of exploiting the information space as society became less susceptible to disinformation, and the available channels to spread disinformation in Lithuania decreased dramatically. Secondly, a rather hawkish stance (albeit not violating European or national laws or norms) has demonstrated the resolve and the will to impose costs if adversarial actions are deemed unacceptable. This stance has been supported by various civil society initiatives, indicating the widespread willingness to respond to unacceptable adversarial behaviour. Lastly, institutional changes, and cooperation between the government, the media and civil society (as well as international cooperation between governments and institutions) has created the agility needed to respond to information threats.

The most recent disinformation campaigns have largely failed to escalate to any great extent. For example, in April 2020, a forged letter purportedly sent by NATO Secretary-General Jens Stoltenberg claimed that Enhanced Forward Presence Battlegroup forces were withdrawing from Lithuania because of Vilnius' inability to cope with the Covid-19 pandemic. This attempt to sow confusion or discord between the international partners via a disinformation campaign was rather easily neutralized before it had a chance to escalate. Capable monitoring and analysis, established partnerships, and the awareness of all parties led to effective strategic communication, as the fake message hardly received any news coverage.[17]

A combination of measures designed to deny benefits but also impose costs – temporary suspensions of Russian TV broadcasts – established precedents that were deemed legitimate by the international courts.[18] This is another important achievement that might serve as a basis for a European-wide response to media manipulation.

As suggested in part 3, the annual surveys do not show any substantial changes in societal perceptions that would raise concerns about a significant Russian information influencing impact. These facts suggest that a strategy which combines governmental, civil and private initiatives, and which includes measures to build resilience, deter by denial and the imposition of costs across different domains can effectively deter hostile activities in the information space. In addition, it can at least reduce and restrict these hostile activities to a more tolerable level, if not totally contain them. This is a key objective of the deterrence strategies in a hybrid environment.

As the discussion on how democratic states can deter hostile actors from using hybrid means continues, the idea that such actors cannot be deterred from employing disinformation should not be taken as axiomatic. Instead, based on the Lithuanian experience in dealing with Russian disinformation since 2014, both thinkers and doers should consider the following:

- **Enhancing legal regulation of the information space.** National and European laws should be enhanced by plugging the loopholes which are being exploited by hostile actors to spread disinformation. Enabling independent regulatory bodies (watchdogs), which act in strict accordance with democratically established rules, is an

17 BNS, 'Provocation against NATO in Lithuania failed, says NATO chief', Lrt.lt, 29 April 2020, https://www.lrt.lt/en/news-in-english/19/1168595/provocation-against-nato-in-lithuania-failed-says-nato-chief. Last accessed 19 April 2021.
18 Vaidotas Beniušis, 'EU court backs Lithuania in Russian TV restriction case', Lrt.lt, 5 July 2019, https://www.lrt.lt/en/news-in-english/19/1075696/eu-court-backs-lithuania-in-russian-tv-restriction-case. Last accessed 19 April 2021.

immensely powerful means of denying access to the targeted audiences and of imposing costs on the hostile actor.

- **Moving from responsive 'crisis communication' to preventive 'strategic communication'.** Gaining ownership of the narrative requires well-established coordination between strategic communicators across governmental agencies (and, further, communicators and the mass media), well-functioning information space/media monitoring, and analysis that includes forecasts on the most probable adversarial information manipulation. A thorough analysis allows one to distinguish between tolerable (low harm) and intolerable activities, and to better allocate limited resources by focusing on those cases which might be most harmful.
- **Broadening the understanding of what constitutes a disinformation threat.** 'Soft power' with toxic content subsidized by the Kremlin and shrewdly targeted at specific audiences is a dangerous tool for shaping the opinion and perceptions of these audiences incrementally. Increased efforts by Russia to craft a biased historical narrative are troubling, as they are deliberately intended to cause tensions between Western allies and partners. Counter-disinformation strategies should not only consider how to respond effectively to immediate disinformation campaigns, but also to slow influencing activities such as these.
- **Supporting and fostering private, civil and non-governmental initiatives that are working on the issue.** Support through financing, providing information, peering, and coordinating is important to avoid duplication and the inefficient use of resources. This can establish a healthy and vibrant ecosystem which promotes whole-of-society counter-disinformation efforts.
- **Looking for hybridity – disinformation is a means to an end, not an end in itself.** In recent years, Lithuania has identified an increasing number of cases where information operations against the Lithuanian authorities have been conducted in coordination with a cyberattack, sometimes with possible consequences on the ground. This requires cross-sector situational awareness and operational coordination in order to mitigate the threats effectively.


Hybrid CoE