Summary of the NATO Riga Strategic Communications Dialogue held on 6-7 May 2021

Author: **Péter TORDA**[1] – 23 June 2021

Introduction

This article summarizes the proceedings of the 5th annual Riga Strategic Communications Dialogue, which was held in a virtual format on 6-7 May 2021 [1][2]. The event was organized by the NATO Strategic Communications (StratCom) Center of Excellence (CoE) in Riga, Latvia.

Summary of the first day (6 May 2021)

In his welcome address, **Jānis Sārts**, the **Director of the NATO StratCom CoE** pointed out that the Covid-19 pandemic has brought to the fore the issue of StratCom. This is exemplified globally by the dumping of Covid-related misinformation and disinformation, which became known as "infodemic", and the heightened risk to information security. He characterized the "infodemic" as a veritable threat to democracy. It was emphasized that StratCom is a global issue and it should be handled as such.

The opening keynote on "**Standing Up to Challenges – Securing the Future of Democracy"** was delivered by **Věra Jourová**, the **Vice President of the European Commission for Values and Transparency**. She stated that contemporary challenges to democracy aim at undermining trust in the democratic system. Increased digitalization makes it easier to attack democracy, not least because on-line media has become the source of information for an increasing amount of people. The Vice President recalled that social media allows disseminating disinformation on an unprecedented scale and with unprecedented precision. She identified disinformation as a major risk to the stability of democracies, as illustrated by pandemic-related disinformation transforming into real-life health risks. The disinformation threat is evolving,

[1] , MA in Security and Defence Policy, MA in European Studies, ORCID ID: https://orcid.org/0000-0002-0087-6518, Email: tordap@gmail.com.

driven in part by foreign actors (Russia was the only one named among them) and by new actors entering the scene. The European Union (EU) has stepped up its work against disinformation in the past years. The Vice President felt that stricter regulation of the on-line space was needed, and she described the proposals made by the European Commission to that effect (e.g. Digital Services Act, European Democracy Action Plans, legislation on sponsored political advertising). The Vice President highlighted the importance of international cooperation in countering electoral threats, including to help prevent foreign on-line interference in elections. She remarked that EU-NATO cooperation is underway on tackling the infodemic as well as foreign information manipulation and interreference. The US has also been mentioned as a key partner. She identified three main avenues of work going forward (1) monitoring and screening of social and traditional media for the spread of disinformation, (2) proper analysis of the information space, (3) action and response through targeted, proactive counter-narratives. In the ensuing interaction with the audience, the Vice President opined that to make societies more resilient, we have to invest in digital education, encourage people to challenge what they read on the Internet, and authorities proactively have to take back the communication space from the disinformers.

A conversation between **Jānis Sārts** and **Jan Havranek Deputy Minister of Defence of the Czech Republic** focused on recent discoveries about suspected Russian actions in the Czech Republic in 2014. This was also presented as a case study of how conflict in the information environment could look like. After the news broke, Russia has speedily responded in the information space: Russian-sponsored websites in the Czech Republic immediately started to spread pro-Kremlin narratives, including to deny the events, to question the authenticity of the Czech government's account, and generally to discredit the whole story. The lesson for the Czech government was that they needed a more coordinated and more robust StratCom capacity at cross-ministerial level. The Deputy Minister pointed out an important question regarding how many conspiracy theories one should try and debunk. The Czech approach to the case in question focused on addressing the (on-line) sources from where disinformation originated so as to stem the spread of disinformation upstream. As regards international support, especially within NATO and the EU, the Deputy Minister perceived clear solidarity among allies and partners. Nevertheless, he considered that multilateral StratCom mechanisms and tools (NATO, EU, G7 etc) would benefit from review in light of how they performed in countering disinformation in this case. Responding to a question on deterrence, the Deputy Minister referred to the issue of strengthening public trust in legitimate state institutions, in which StratCom plays a crucial and continuous role.

A **panel discussion** entitled **"Global Pandemic Turned Infodemic? Tackling the Threat to National Security"** took place with the participation of academics and practitioners as well as an official of the World Health Organization (WHO). It was suggested that the pandemic has directed more attention to (strategic) communication than ever before, and this will probably entail a rethinking of the role of StratCom post-crisis. The Russian-mounted "vaccine war" disinformation campaign, which aimed to discredit Western-produced vaccines and promote the Russian-produced one, was discussed in relation to its effects among Russian-speaking populations in Estonia, who are more exposed to Russian narratives. As a lesson, the importance of targeted communications was underlined, which means adapting the narrative to different segments of the population so as to get the core message across. One panelist elaborated on the "anti-vaccine industry", which predates the Covid-19 pandemic, and is specialized in spreading disinformation about vaccines and in sowing distrust in the health system on a large scale. These anti-vaccine organizations concentrate on social media to recruit followers, and they do so with absolute impunity. These organizations are economically motivated, e.g. selling merchandise on-line and collecting participation fees for "anti-vaxxer" events. A panelist addressed the phenomenon of motivated denial of science (a more accurate description of "science skepticism"), which manifests itself in different forms, from tribal superstition to political extremism. There is a correlation between espousing extreme ideologies and science denial, and when it comes to "anti-vaxxer" conspiracy theories, this behavior is more typical on the extreme right than on the extreme left. It was argued that preventive "psychological inoculation" against disinformation is more effective than debunking and fact-checking after disinformation has mentally taken hold. For instance, the controlled introduction to people of on-line manipulation strategies, or "pre-bunking", could be a way to achieve "psychological inoculation". There have been experiments of "pre-bunking" through games and animated videos to make it more attractive to audiences. The Director of the WHO Regional Office for Europe considered that misinformation and distrust are among the greatest security threats of all time. The Covid-related infodemic has been deepening and lengthening the health crisis, triggering a massive impact in the real world ("biological warfare waged through information warfare"). The Director recalled that abusing the information space is not new: the term "fake news" has been in use since the 1920's, and the term "infodemic" was coined in 2003. However, in the digital age, disinformation spirals across the world faster than a virus can. This means that effective communication has become a crucial public health intervention.

In his keynote, **Mircea Geoana**, **NATO Deputy Secretary General**, confirmed that NATO is actively addressing the threat of disinformation. The pandemic has amplified this threat, with more and more sophisticated occurrences of disinformation campaigns, cyberattacks and online espionage. NATO will continue to invest in StratCom capabilities to meet the challenges of a highly contested communications space, both at the level of the Alliance and of allied nations. The Deputy Secretary General underscored the importance of proactive communication on all wavelengths, including media engagement, digital communications, face-to-face events and social media, so as to make sure that everybody hears NATO's story first. The proposed NATO 2030 vision, inter alia, sets clearer and more measurable national resilience targets, including in the field of communications. The Deputy Secretary General posited that on the way forward it will be key to invest in StratCom, to conduct proactive communications, to build societal resilience and to cooperate with like-minded partners (EU, G7, United Nations and others).

A panel discussion on **The Future of Democracy – New Understanding of Free Speech and Responsibility?** brought together a Swedish government minister and academics. The discussion revolved around the controversy of managing the digital revolution and exhausting its tremendous potential to broaden democratic participation, while tackling the challenge of disinformation on-line. This means striking a subtle balance between defending free speech and defending against the risks of disinformation in the on-line realm, including the risk of provoking real-life violence (the attack on the US Capitol on 6 January 2021 was cited as a headline example for the latter). The speed and spread of disinformation, as well as access to it, has been steeply on the rise in the recent period. There was a shared understanding across the panel on the need for better regulation of global social media platforms as well as on the need to better regulate manipulating and intimidating behaviors in the on-line space. Self-regulation of social media platforms was seen to come late and show significant incoherencies across the sector. However, it was also pointed out that the majority of states who have so far adopted measures against disinformation and fake news tend to have authoritarian tendencies (Russia and China were specifically mentioned), which raises the suspicion of ulterior motives of curtailing free speech. The panel agreed that the present state of affairs in the on-line domain requires new types of responses from governments and multilateral organizations, where cooperation with technology companies will be indispensable. A panelist from academia struck a more urgent note, considering that the "democratic community" had a shared recognition on the necessity of regulation, without a shared gameplan on how to act on it (i.e.

putting in place internationally coordinated regulatory policies). The exchange touched upon the issue of "freedom of speech vs. freedom of reach", meaning that the right to freely express oneself does not necessarily imply the right to propagate one's message without any limitation (cf. former US President Trump's ban from Facebook and Twitter). While a panelist from academia appeared more insistent on regulation in this regard, the Swedish government minister emphasized the paramount importance of upholding freedom of speech. Panelists shared the view that media education can play an important role in strengthening people's defenses against manipulation.

In her keynote under the title "**The Key to Ending the Infodemic Is Empowering The People"**, **Kaja Kallas** the **Prime Minister of Estonia** illustrated the scale of the infodemic by recalling that between March and October 2020, Facebook alone removed more than 20 million pieces of Covid-19 related misinformation and added warning labels to 167 million Covid-19 related posts. She considered that the functioning of democracies depends on the ability of citizens to make informed decisions, especially in times of crises. She recalled that the pandemic has amplified existing trends in disinformation. These include vaccine skepticism (which is as old as vaccines themselves) as well as the trend of foreign interference combining with domestically produced disinformation, spread for personal, financial or political reasons. The central message of the Prime Minister was that key to ending the infodemic is empowering the people and thereby increasing the resilience of societies and reinforcing trust in democratic institutions. The Estonian approach focused on increasing awareness raising and enhancing media literacy, diversifying the range of information channels available to people and on empowering the voices of authentic experts. On the question of reaching audiences who are isolated in their own "information bubbles", the Prime Minister referred again to improving media literacy so that people become more source critical. In terms of the adequacy of existing international cooperation mechanisms to deal with the infodemic, the Prime Minister expressed satisfaction with cooperation at European level, but felt that global cooperation to tackle the infodemic could be improved.

Summary of the second day (7 May 2021)

A panel discussion on **"Setting Standards and Rules for a Safer Digital Environment"** brought together a Member of European Parliament (MEP), the EU Representative of Facebook and regulators from the Australian

Communications and Media Authority. In Australia, the basic approach of the regulator is to encourage self-regulation by the industry, under the guidance and monitoring of the authority. It was recognized that the biggest digital platforms, such as Facebook and Google, played an increasingly important role in determining news and journalistic content in the country. Therefore, the regulator prompted all major digital platforms to develop an industry code of practice, which addresses concerns around disinformation and news quality. Facebook and Google were further invited to develop a code to address the imbalance between their platforms and news publishers. Moreover, an industry-initiated Disinformation and Misinformation Code was released with the largest on-line platforms among its signatories. The importance of international regulatory collaboration was also underlined from the Australian perspective. The MEP elaborated on relevant legislative proposals currently examined by the European Parliament (EP): the Digital Services Act to better counteract illegal content; the Digital Markets Act to govern the most powerful on-line platforms; and a complex regulatory framework for Artificial Intelligence (AI). From an EP point of view, cooperation with the US is deemed crucial to defend against on-line challenges to the democratic system, notwithstanding differences between European and US approaches on certain issues, e.g. data protection or the issue of an international digital tax. The MEP argued that addressing disinformation through industry self-regulation, i.e. the approach currently proposed by the European Commission, is insufficient. Obligatory European legislation was seen necessary in this regard. The Representative of Facebook agreed that self-regulatory initiatives are not enough, and private companies should not be "left alone" with politically charged decisions, such as the balance between free expression and suppressing harmful content. At the same time, she underscored the democratic dividend of social media in terms of democratic participation and accountability. It was recurrently emphasized that Facebook does not benefit from hate speech in any way, and has a strong interest in stepping up against it. In terms of political advertising, Facebook is looking at the EU for clearer guidance, with the added complication of electoral rules falling under the respective competences of 27 EU Member States. Facebook reported on what they termed as fundamental changes in their practice with a view to breaking up "echo chambers" and "bubbles" which expose users to self-perpetuating narratives. Also, Facebook's algorithms now prioritize posts by friends and families, and users can tailor-make their news feeds.

In his address on **"The Future of Technology – the Future of Society"**, **Egils Levits**, the **President of Latvia**, underlined that technology has to be aligned with democratic principles and not vice versa. He noted that the global situation of democracy is backsliding, and one reason is the harmful side of technological development. The President stated that the adversaries of the "democratic world" employ technological means, among other things, to weaken democracies. Regarding the European Commission's proposed Digital Services Act, the President shared the view already voiced in the previous session that digital platforms should not be left to self-regulate content, as such competence is for legitimate state authorities. On the question of how much autonomy we should give to AI to control content, the President opined that technology can only help, but not replace human decisions. The President argued that big Internet platforms should be regulated in a particular way, in proportion with their profound reach through society.

In his **"Strategy Talk on Re-discovering the Cognitive Battlefield: What next?", General Paolo Ruggiero**, **NATO Deputy Supreme Allied Commander Transformation**, pointed out that in recent years the cognitive dimension has come to the fore of military thinking. The reason is that potential adversaries have increased their capacities to target the cognitive domain. The objective of such operations in the cognitive battlefield is to covertly degrade capacities for knowledge and to exploit the vulnerabilities of the human mind. Response and retaliation entail important dilemmas in the cognitive domain. The General clarified that in contrast with propaganda (which aims to influence "what" people think), cognitive warfare aims to influence "the way" people think, e.g. by undermining trust in the democratic system. Cognitive operations combine real and distorted information, exaggerate facts and fabricate news to amplify pre-existing social and political confrontations and to create divisions and frustrations. Also, there is no clear end point to cognitive warfare. Russia and China have both developed their capacities for cognitive warfare, particularly through disinformation, deception and fear. Russia has prioritized cognitive operations as precursor to the kinetic phase, while China more broadly defines cognitive warfare as "the systematic use of cognitive science and biotechnology to achieve mind superiority". The rise of neuroscience and the rapid expansion of emerging technologies might offer infinite possibilities to exploit human cognition, i.e. to manipulate brains, perceptions and therefore thoughts and behaviors. The cognitive dimension will only become more complex, putting a prime on building resilience and capacities in this area. Against this background, the General underlined the unique contribution of NATO's StratCom capacities, and highlighted that NATO is currently working on an initial concept for the cognitive domain. Responding to questions, the General considered that StratCom forms part of NATO's activities in all domains, and it will only grow in importance.

The line-up of the panel debate on **“Deterrence of the 21st century – New Challenges vs Old Thinking”** included the Foreign Minister of Lithuania and academics. The Minister considered that Russia is becoming more aggressive by the day, and expanded on Russian influencing and disinformation campaigns against “the West”. The Minister held that countering disinformation and foreign interference in the information space should be built on a comprehensive strategy and policy, encompassing credible deterrence. He argued for a forward-looking disinformation strategy based on political determination, partnerships with the private sector and civil society as well as enhanced media literacy and strong resilience to withstand attacks. The aim is to change the calculation of disinformation actors, as disinformation so far has been a “low risk – low cost – high reward” activity. Measures to raise costs – such as sanctions, denial of capabilities and the exposure of instigators – could change the calculation. The Minister considered that the Lithuanian practice proves the worth of deterrence through early warning, reinforcing societal resilience, and adaptive legislation. In terms of countering disinformation campaigns, the Lithuanian state response was greatly reinforced by civil society. Panelists from academia pointed out that deterrence in the cyber domain is more complicated than in the kinetic domain. On the one hand, the responses to known Russian cyberattacks (against the US) were not seen to have a deterrent effect. On the other hand, we have not seen any cyberattacks which caused major societal disruption – and this may have been due to effective deterrence, even though difficult to evidence. The question remains how the logic of deterrence applies in the hybrid and cyber domains. In these domains, clarity and attribution tend to be more fluid, whilst clear attribution is a precondition to credible deterrence. Also, the risk of “hacking back the aggressor” does not seem to deter cyberattacks. Another question relates to deterring non-state actors, which is coming back to the center of attention in regard of cyberspace (it used to be a trending issue in relation to terrorists). Reinforcing resilience was identified as probably the best measure to deter against “grey zone” attacks, as it decreases the expected reward in the eyes of the potential aggressor. It was argued that StratCom is at the essence of deterrence as a means to tangibly convey the message of deterrence and shape perceptions accordingly. Addressing the role of StratCom in NATO’s deterrence, one academic distinguished between (1) general deterrence, which includes indirect messages (e.g. political unity, capability, willingness to act, exercises, deployments), direct messages (ability to fight and prevail in conflict) and messages to reassure own populations; and (2) deterrence in a crisis mode, which supposes getting across messages in acute situations, in a congested and contested information space. It was felt that StratCom may fail to live up to the requirements of operating in crisis mode, and in those situations more traditional channels of diplomatic and political contacts may become dominant.

A panel discussion on "**Living Smart with AI, Big Data & Emerging and Disruptive Technologies"** took place with the participation of a Minister of State from France, a US Presidential Advisor as well as experts. The French Minister of State described two disconnects: one between innovation and productivity (productivity grows at a much slower pace than innovation) and another between innovation and progress (people do not see tangible benefits of innovation in their lives). Addressing the problem of regulating the digital space, he warned that regulation in democratic countries inevitably lags behind governance in authoritarian systems. He underscored the centrality of multilateral governance in managing the globalized digital domain. The US Presidential Advisor remarked on the complications of helping citizens understand the impacts of AI, arguing that a framework still needs to be developed for effective communications about AI matters. The oversight of the technology sector emerged as a key issue in the panel discussion. From a communications perspective, it was pointed out that humanity's traditional constraints on disseminating information have largely disappeared: in today's world, one can virtually communicate with anyone and anywhere without limitations. There are serious questions about the "if" and "how" of constraining such boundless communication. There was a shared view across the panel that technology and innovation have progressed far ahead of the regulatory framework. Experts on the panel saw serious trust issues involved in AI: delegating formerly human-controlled work to AI means surrendering responsibility and diluting accountability. It was expected that the regulatory gap between the European Union and the US in terms of regulating the technology sector will narrow in the future, meaning more stringent regulation on the US side. Regarding self-regulation by the technology sector, an observation was expressed about the unelected and unaccountable nature of technology companies' decision makers, in contrast with public decision-making.

In his concluding remarks, **Jānis Sārts** the **Director of the NATO StratCom COE** stressed the risks of applying old thinking to new challenges and the resultant need to adapt to new realities. He underscored that the present operating environment as well as the course of its evolution remain uncertain, and actors have to operate within uncertainties. He concluded that NATO is embracing this new reality, and working to adapt to it. The Director recalled that militaries alone cannot meet the challenges of the day, and the whole of society needs to become resilient to these challenges, not least through day-to-day investment into protecting democracy. It was seen as promising that regulation of the digital environment is accelerating on both sides of the Atlantic. He considered it crucial to address the trust deficit afflicting societies. The Director also found it apparent that the nature of conflict is broadening, and the cognitive domain needs seriously to be addressed. The centrality of StratCom to deterrence was underlined.

References

[1] Recordings of the Riga StratCom Dialgoue 2021 sessions. Available: https://www.youtube.com/playlist?list=PL6ljTZ2XuHJ6WmSdW40KvzQBA5IAmUMBt (Accessed: 21 June 2021)

[2] Agenda of the Riga StratCom Dialgoue 2021. Available: https://rigastratcomdialogue.org/agenda/ (Accessed: 21 June 2021)