NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMITTEE ON DEMOCRACY AND SECURITY (CDS)

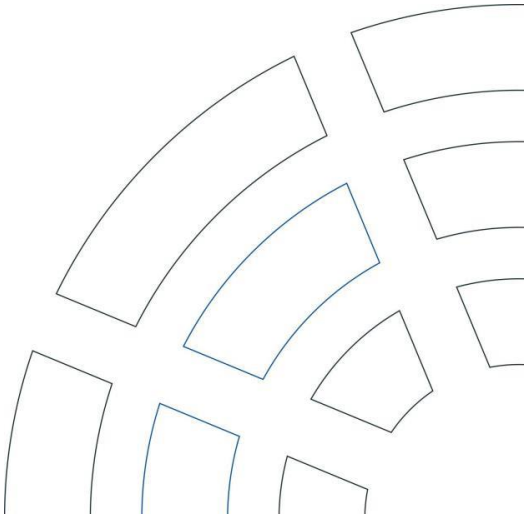
THE RUSSIAN WAR ON TRUTH:

DEFENDING ALLIED AND PARTNER DEMOCRACIES AGAINST THE KREMLIN'S DISINFORMATION CAMPAIGNS

General Report
Rodrigue DEMEUSE (Belgium)
Acting General Rapporteur*

014 CDS 23 E rev.2 fin – Original: French – 8 octobre 2023

* *The report was originally drafted by Joëlle Garriaud-Maylam (France), CDS general rapporteur until 1 October 2023. Mr Demeuse kindly agreed to present the revised version on behalf of Ms Garriaud-Maylam to the Committee.*



EXECUTIVE SUMMARY

Russian disinformation poses a serious threat to the security and democracy of Euro-Atlantic area countries. By eroding the distinction between reality and fiction, the Kremlin and its supporters seek to amplify societal divisions and destabilise Allied and partner states. They also seek to undermine citizens' trust in democratic institutions and systems.

The Alliance has taken concrete steps in recent years to build resilience to these malicious attacks in the information space. However, given the growing scale and severity of the threat, the Euro-Atlantic community and its partners must now redouble their efforts to better protect their societies.

The aim of this general report is to stimulate avenues of thought to aid in this fight. It delves into the origins, recent developments, objectives and operations of Russian disinformation. Additionally, it provides an overview of the various measures taken by Allied and partner nations to counter it and examines the reasons behind Ukraine's success in combatting Russian information manipulation during the new invasion. Finally, it sets out recommendations for Allied governments and NATO to develop a more cohesive and efficient response to Russian disinformation.

TABLE OF CONTENTS

I- INTRODUCTION

1. The threat of Russian disinformation is a grave concern for Allied nations and their partners. Although this threat is not new, it has escalated with the emergence of new information and communication technologies. The Kremlin has adapted its strategies to the increasingly digital and open environments of Allied and partner societies, while drawing on methods used during the Soviet era. Furthermore, it has learned from past failures in manipulating information.

2. Disinformation, or "the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead" (NATO, 2020), has become a key component of Russia's political and military arsenal. Over the past few decades, the Kremlin has frequently employed disinformation to support its destabilising and imperialist foreign policy.

3. Starting in February 2022, Russia launched an onslaught of fake news and manipulative narratives as part of its illegal and unjustifiable invasion of Ukraine. These despicable tactics have multiple aims: to demoralise the Ukrainian people and weaken their resolve to resist; to cover up atrocities committed by Russian troops while accusing Ukrainian soldiers of fabricated violations; and to gain public support in democratic countries by justifying unlawful aggression with cynical lies. However, the courage and determination of the Ukrainian people in resisting the invasion and the strong and widespread support they have received from the Alliance and beyond demonstrate that Russian disinformation has failed to achieve its goals.

4. The Kremlin's continued hostility in the information space nonetheless remains a major security risk for Euro-Atlantic countries and neighbouring regions. In spreading falsehoods, Russian disinformation actors aim to weaken Allied and partner states by sowing discord, promoting social divisions and even inciting social and political unrest.

5. Russian disinformation is also a threat to democracy. The Russian propaganda machine frequently targets the processes and institutions at the core of democratic societies to undermine their legitimacy. Even more alarmingly, it attacks the fundamental principles of democracy. It exploits and misuses freedom of expression to flood the world with a rapid and continuous stream of lies, thereby challenging the very possibility of objective, factual information. Yet trust in the media and informed decision making are the foundations of democracy. By blurring the line between reality and fiction, the Kremlin and its supporters seek to snuff out the flame of democracy. Even within Russia, the regime is drowning the population in a deluge of lies and repression to ensure its own survival.

6. Although the Alliance has taken concrete steps in recent years to strengthen its information resilience, the scope and severity of the security and democratic threat posed by Russian disinformation are growing. The Euro-Atlantic community and its partners must therefore intensify efforts to better protect their societies. This report, which continues the work initiated by the Chair of the Committee on Democracy and Security, Linda Sanchez (United States) in 2021 (Sanchez, 2021), aims to provide avenues for reflection to contribute to this effort.

II- THE ORIGINS AND EVOLUTION OF CONTEMPORARY RUSSIAN DISINFORMATION

A. THE HERITAGE OF SOVIET "ACTIVE MEASURES" AND ADJUSTMENT TO NEW DIGITAL TECHNOLOGIES

7. Moscow's use of information manipulation is a long-standing tactic. The Bolsheviks first established a bureau in 1923 to carry out such operations abroad and disinformation soon became a key element of the Soviet political and military toolbox (Richter, 2019). It was a central element in the regime's "active measures", which included a range of conspicuous and clandestine subversive activities, from political assassinations to the incitement of social unrest (Pynnöniemi and Rácz, 2017; Galeotti, 2019).

8. Their primary goal was to promote communist ideology and spread a positive image of the Soviet Union. The regime's efforts at information manipulation were mainly focused on advancing political, anti-colonial and social causes within democratic societies. As Anne Applebaum noted, disinformation campaigns aimed to "dismantle the enemy before you have to fight with the enemy" and "disarm and undermine the West" at a low cost and below the threshold of armed conflict (Cray, 2022). Soviet disinformation thus sought to influence Allied and partner state leaders and public opinion, disrupt state relations, undermine citizens' trust in democratic institutions and discredit opponents of communism (Pynnöniemi and Rácz, 2017).

9. After the dissolution of the Soviet Union, Russia continued to use information manipulation for subversive and destabilising purposes. The Kremlin's tactics and some of its objectives in this area remain fundamentally the same today. In many ways, contemporary Russian disinformation thus has its roots in Soviet disinformation, but its methods and tools have evolved. The Soviet-era Kremlin propagated false or distorted information at home and abroad through radio, television, newspapers, organisations and individuals dedicated to the communist cause. Today, while still spreading disinformation through mainstream media, Russia has also embraced recent technological developments.

10. Since the early 1990s, it recognised the potential of new information technologies both as a tool for dissemination and a fertile ground for disinformation activities (Giles, 2017). The emergence of the internet and social media democratised access to information and gave citizens new ways to express themselves. However, it has also allowed those who create and spread disinformation to reach a large audience easily, freely, directly and in real time. These actors enforce their messages by exploiting the ubiquity and anonymity of the internet and social networks especially.

11. Russia is still adapting to emerging technologies and incorporating them into its arsenal of disinformation tools. In particular, the Allies must heighten their vigilance with regard to the Kremlin's potential use of artificial intelligence to create and disseminate increasingly convincing and widespread disinformation. The deployment of artificial intelligence systems trained to produce original written content or capable of creating false audio and visual materials (deepfakes) has the potential to inundate and erode the information space (Goldstein and Sastry, 2023).

B. THE CONSTANT EVOLUTION OF INFORMATION MANIPULATION AS A DESTABILISATION STRATEGY

12. The Russian approach to disinformation is continually evolving, often as a response to the Kremlin's failures in this area, particularly in the 1990s and early 2000s. During the first Chechen War, Russia struggled to control the narrative being constructed in Russian and foreign media about its offensive. The Russian defence minister at the time described the government's performance in this area as "the quintessence of helplessness" (Giles, 2016). The Kremlin partially altered its approach during the Second Chechen War by severely restricting journalists' access to the region and establishing a single centre for disseminating information about the war (*Rosinformcenter*) to organise and shape media coverage of the conflict as it saw fit (Gordon, 1999).

13. However, the Russian government and military only fully recognised the importance of information control and manipulation during the war with Georgia in 2008. This was the first conventional Russian operation abroad conducted in conjunction with modern information manipulation operations (Giles, 2016). The disinformation spread by the regime during this time had some success among the Russian population, primarily due to their limited exposure to information sources that did not repeat the Kremlin's line. But abroad, Russian disinformation did not take root. As a result, the Russian authorities invested in new human and technical capabilities to conduct disinformation operations after the war, including targeting non-Russian-speaking foreign audiences (Giles, 2016a).

14. Since then, the Kremlin's realisation that it cannot match NATO's conventional military capabilities has led it to increasingly rely on information manipulation as a tool for political and military influence. In 2013, this position was codified in the Gerasimov Doctrine, named after the Russian Chief of General Staff who developed it. According to the doctrine, the information space is a grey zone where the distinction between war and peace does not apply, allowing Russia to freely, persistently and effectively carry out non-military hostile actions. Disinformation is a key aspect of Russia's hostile informational activities, albeit not the only one (Giles, 2016b; McKew, 2017).

15. The importance of disinformation as a weapon in its own right was then demonstrated during Russia's unlawful annexation of Crimea and forcible takeover of parts of the Ukrainian regions of Luhansk and Donetsk in 2014. Before the arrival of Russia's "little green men" in Crimea, the Russian military intelligence service (GRU) conducted a massive disinformation campaign to sway policymakers and public opinion in these regions. The operation involved paying individuals to create fake social media accounts and deceive people into believing that most Ukrainians opposed the Maidan Revolution (Nakashima, 2017).

16. Since February 2022, just before and during its latest invasion of Ukraine, Russia's disinformation campaigns in this country and beyond have marked a further escalation in its use of information operations (OECD, 2022). These efforts were largely fruitless, both in Ukraine and within the Alliance. Nonetheless, such operations pose a significant threat to democratic countries as they become more sophisticated and intense (Tokariuk, 2023). It is thus crucial to learn from Russian disinformation failings, Ukrainian resilience, and Allied success in countering these operations since the start of the latest invasion.

17. Much as in Soviet times, the Kremlin sees itself as engaged in a permanent, total and global conflict in the information space. The disinformation campaigns it leads across multiple theatres of operation, in the Middle East, Africa and Ukraine, demonstrate its desire to destabilise NATO and its Allies on a global scale. In contrast, Western countries and NATO view information operations as tactical and limited actions carried out in the context of conventional conflict, responding to disinformation with verified and objective facts, rather than resorting to the dissemination of false information (Giles, 2016b). Russia, meanwhile, has much broader, more persistent and destabilising objectives.

III- THE MAIN OBJECTIVES PURSUED BY THE KREMLIN IN THE INFORMATION SPACE

A. DIVIDING ALLIED SOCIETIES TO DESTABILISE THEM

18. Unlike during the Soviet era, Russian disinformation aimed at the West does not seek to promote the superiority of its authoritarian model or the merits of its policies. Rather, its primary objective is to weaken democratic societies and increase Russia's relative power. To this aim, Russian disinformation actors exploit existing fault lines in Western societies, such as ethnic, linguistic, regional, social and historical divisions, and amplify divisive narratives.

19. One of the Kremlin's strategies is to manipulate information and thereby erode consensus among Western populations and leaders on the security, moral and democratic imperative of supporting Ukraine in its resistance to renewed Russian aggression. For instance, in August 2022, Russian media and pro-Kremlin social media accounts disseminated a doctored video of German Foreign Minister Annalena Baerbock, falsely claiming that she prioritised supporting Ukraine over the interests of her own electorate. The video was viewed thousands of times within a few hours, and a hashtag calling for the minister's resignation gained popularity on Twitter (La Cour, 2022).

20. Russia also employs disinformation as a means of undermining the global standing and perception of Western democracies. Its approach hinges on fostering distrust, capitalising on historical grievances, and aligning with anti-Western and anti-democratic movements. This strategy finds resonance in multiple nations across Africa, South America and the Middle East, where Russia seeks to expand its influence and mobilise diplomatic support for its latest illegal invasion of Ukraine (The Economist, 2022a).

B. UNDERMINING AND DELEGITIMISING DEMOCRACY

21. One of the objectives of Russian disinformation is to erode public trust in electoral systems and democratic institutions. Such disinformation campaigns carried out by the Kremlin pose a major threat to democracy (Sanchez, 2021).

22. The 2016 US presidential election serves as an example of how Russia used information manipulation to undermine the legitimacy of an electoral process. The US Office of the Director of National Intelligence (ODNI) released a declassified report stating that after hacking into the Democratic National Committee and Hillary Clinton's campaign manager's e-mail accounts, the GRU created a fake digital persona and website to leak their e-mails (Sanger, 2017). Similarly, according to several analysts, Russia attempted to influence the 2017 French presidential election by launching a sustained disinformation campaign months before the vote. This culminated in the hacking of e-mails linked to Emmanuel Macron's campaign, which were leaked together with fakes two days before the second round of the election. Russian news channels and an army of fake social media accounts then disseminated these e-mails (Jeangène Vilmer, 2019).

23. Such hacked accounts belonging to public figures are frequently leaked through popular online forums. This technique of disseminating information through unofficial channels makes it harder to trace its origin and thus helps it spread more widely. Russian operatives also rely on real individuals in the US and Europe to pass on the alleged inside information, either knowingly or unwittingly. The combined use of both verifiable and fake accounts to spread this information further blurs the truth.

C. USING LIES AND REPRESSION AS A SURVIVAL TACTIC

24. Moscow views information as a double-edged sword. When manipulated by the Kremlin, it becomes a powerful means of destabilisation to further its interests. However, if it exposes the truth to the Russian public about the regime's illegal and unacceptable policies and endemic corruption, it poses a significant threat to the Kremlin's existence.

25. In response to this potential challenge and to prevent dissent, the Russian leadership has steadily gained control of the country's media landscape since the 2000s. Much like in the Soviet era, Russian media now serves as a propaganda machine to mislead the population. Most media outlets have been acquired by individuals who support the regime, and the main television channels, which are the primary sources of information in Russia, broadcast the Kremlin's narrative throughout the day. The same is true of the vast majority of newspapers and radio stations (Gessen, 2022a).

26. Most Russians thus have limited access to independent sources of information. The law on "foreign agents" enacted in 2012 is often used to target journalists, media outlets and organisations that are perceived to be opposed to the regime. Any remaining independent media organisations are continuously pursued through the legal system, intimidated and harassed (Denber, 2022). Moreover, restrictive legislation makes it difficult to access social media and foreign sources of information.

27. By limiting the information space, the regime can disseminate false information to the Russian population, with the aim of ruling unopposed and ensuring its own survival. Such forced informational isolation prevents Russians from fully recognising the regime's duplicitous messaging and keeps them politically disengaged. Similarly, Allied countries find it more difficult to counter false claims spread against them in Russia. For instance, Russian media frequently rely on false information to promote the Kremlin's message that Western countries disrespect Russia, intend to humiliate it, and pursue aggressive and expansionist policies towards it, without the fallacy of these stories ever being exposed (Lough, 2021).

28. The Kremlin also employs its internal disinformation campaigns to manipulate Russian historical narratives, with the same goal of unfettered governance and political survival. The regime's media outlets constantly echo its rhetoric, portraying the darkest moments and personalities of Soviet history, including Stalin and the Holodomor genocide, in a positive light. Even school textbooks are censored and edited to align with the official version of the Soviet past (Becker and Myers, 2014). The regime labels any opposition, both domestic and foreign, as "fascist" or "Nazi" (US State Department, 2022a). It uses the pretext of fighting fascism to justify the most reprehensible actions of its aggressive and imperialist foreign policy, including the war against Georgia, the latest invasion of Ukraine, the annexation of Crimea and the takeover of parts of Ukraine's Luhansk and Donetsk regions.

29. The Kremlin's utterly false and misleading geopolitical and historical narratives aim to evoke feelings of patriotism and nostalgia among the population by inventing a righteous and ideological national struggle against an internal and external enemy. The regime presents itself in the Russian media as the only credible bulwark against this imaginary threat. This disinformation campaign reinforces the regime's credibility and support among the population while discrediting its opponents as enemies of the state (Persson, 2020).

IV- THE MULTIPLE ACTORS AND STRATEGIES OF RUSSIAN DISINFORMATION

A. AN ECOSYSTEM OF LIES

30. Russian disinformation is created and spread by many different actors, forming a complex ecosystem with several main components. The first includes **official representatives and organisations**. The Kremlin, members of the Russian parliament and foreign ministry staff, along with other figures, frequently peddle manipulated or false information and conspiracy theories through social media posts and official statements. **Intelligence agencies** also play a crucial role in organising and amplifying the Kremlin's disinformation operations. They seek out and fabricate incriminating information about the regime's opponents, recruit individuals, organisations and public figures to promote the authorities' false narratives, and work to sow division and chaos in democratic countries (Watts, 2018). They also monitor the Russian internet to prevent access to information not approved by the Kremlin and to silence any opponents who circulate it (Mozur et al., 2022). Lastly, since Putin came to power, they have largely silenced Russian media by harassing, convicting and even assassinating journalists who refuse to toe the Kremlin's line.

31. The most visible participants in the dissemination of Russian disinformation abroad are its **state-sponsored media outlets**. These major media companies have either implicit or direct ties to the Kremlin. They own and manage numerous television channels, radio stations and websites aimed at non-Russian-speaking audiences. *RT* (formerly *Russia Today*) and *Sputnik* are the most well-known outlets, broadcasting in over 30 languages and receiving USD 1.3 billion per year in state subsidies to disseminate a constant flow of false information globally (Lomas, 2022; US State Department, 2022b). These two media sources also have a disconcerting level of success on social media. For example, in 2017, *RT* had no less than 2.2 million subscribers on its YouTube channel (Wakabayashi and Confessore, 2017). Shortly after the start of the new Russian invasion of Ukraine, the UK, Canada and the EU banned the broadcasting of *RT* and *Sputnik*, and *RT*'s US service ceased to operate. However, *RT* is still accessible in the rest of the world and continues to spread disinformation.

32. Other Russian sources of disinformation flood the internet with fabrications through **troll factories** (fake accounts on social networks run by people who are often paid to do so) **and bots** (automated fake accounts). The *Internet Research Agency*, founded in 2013 by a Russian oligarch with close ties to Putin, is the most well-known participant in this field due to its involvement in the Kremlin-led disinformation campaign during the 2016 US presidential election (Volchek, 2021).

33. The Kremlin relies on **various other actors** to promote its disinformation. Some online publications and websites based abroad conceal their ties to Russia to better amplify its disinformation campaigns. The sprawling ecosystem of Russian disinformation also includes organisations catering to the Russian and Russian-speaking diaspora, such as *Rossotrudnichestvo* and the Russian World Foundation (*Russkiy Mir*), think tanks like the Valdai Discussion Club, and private military companies such as the Wagner Group. The Kremlin also uses the Russian Orthodox Church as a catalyst for its false narratives, both at home and abroad, and especially in Ukraine (O'Beara, 2022). In addition, religious, educational and cultural bodies, political parties and figures, as well as supposedly independent civil society organisations, propagate the Kremlin's untrue accounts of events. The regime even endorses those acting as pro-Russian journalists to serve its disinformation campaigns. For instance, while the Russian government severely restricted foreign journalists' access to the Ukrainian regions of Donetsk and Luhansk, which have been under its illegitimate control since 2014, it has facilitated access for media personalities sympathetic to its cause to spread lies in Western countries.

34. By co-opting these actors to spread false information, the Kremlin makes its disinformation harder to identify and gives it greater visibility among citizens of targeted countries (Lucas and Pomeranzev, 2016). These citizens, in turn, become vectors for the dissemination of Russian disinformation within democratic societies, even though they are not strictly speaking part of the Russian ecosystem. For the most part, they are unwittingly spreading false information springing from Russian sources. This is partly due to the abundance of online information, particularly on social media, and an insufficient capacity to detect disinformation (Sanchez, 2021).

B. CHARACTERISTICS AND STRATEGIES OF RUSSIAN DISINFORMATION

35. All the actors within the Russian disinformation ecosystem are helping the Kremlin to spread its propaganda and achieve its objectives. However, this ecosystem operates more like a **decentralised network of autonomous entities that echo each other**, rather than a closely coordinated and hierarchical structure. The Russian approach to disinformation does not involve the authorities actively coordinating the promotion of specific narratives. Instead, the different actors operate independently, but not in isolation. They spread disinformation by interacting and cooperating with each other, echoing, expanding and amplifying each other's false information and manipulated narratives. This constant **repetition** plays a central role in disseminating Russian fake news, making it louder and more visible (Watts, 2018; US State Department, 2020).

36. Misleading and manipulative narratives overlap, forming a formidable torrent that floods the information space and overwhelms the target audience. The **overwhelming speed** at which this occurs is another main characteristic of Russian disinformation. Russian media outlets rapidly cover events to occupy the information space and be the first to spread their manipulative interpretations. In the age of immediate and continuous access to information, the speed at which Russia spreads its lies makes it challenging for conscientious media, which must take the time to fact-check to effectively counter it (Paul and Matthews, 2016). Social networks and online forums further speed up the spread of false information, as these platforms are often insufficiently moderated, if at all. There is a significant risk that the Kremlin will leverage the ongoing advancements in artificial intelligence to bolster its capacity to inflict harm in this domain.

37. The **deliberate lack of coherence** is one of the most perplexing features of Russian disinformation. Its promoters shamelessly saturate the information space with conflicting assessments and even absurdities. For instance, the Kremlin can label the Ukrainian army and leadership as Nazis while accusing them of being involved in a global Jewish conspiracy (Snyder, 2022). Moscow has also made unfounded accusations against Poland for allegedly preparing to annex western Ukraine, while flouting international law by invading from the east (Salvo, 2022). Similarly, it has falsely accused Moldova of considering the use of force against its own region of Transnistria, while also challenging the country's territorial and democratic integrity (Reuters, 2023). Unlike the Soviet disinformation that strived to be viewed as reliable and fact-based, its modern Russian equivalent makes no such efforts. Instead, it shamelessly exploits and misuses the fundamental democratic principles of freedom of expression and access to information to undermine citizens' belief in objective information. Yet trust in the media and informed decision making are essential pillars of democratic societies.

38. By attacking information, the Kremlin is attacking democracy, which is why **other authoritarian states support Russia** in its efforts to manipulate information. To undermine democracy and promote their repressive models on a global scale, these states join forces to spread their respective disinformation campaigns. For example, Chinese state media spread Kremlin disinformation about the latest aggression in Ukraine, repeating absurd claims that President Zelenskyy is a puppet of the billionaire George Soros, or that there are US biological weapons in Ukraine (Dwoskin, 2022; Bandurski, 2022). Russia reciprocates by amplifying Chinese narratives denying human rights violations and repression against Uighurs in Xinjiang province (EUvsDisiNFO, 2021a). Russia and Iran are also cooperating in this area. For instance, Iranian and Russian

disinformation actors have worked in tandem to discredit the Syrian voluntary relief organisation "White Helmets", refute the use of chemical weapons against civilians by the Syrian regime, and denigrate investigations into these attacks (EUvsDisiNFO, 2021b; Uddin, 2022).

V- RUSSIAN DISINFORMATION IN THE CONTEXT OF THE RENEWED INVASION OF UKRAINE

A. WHEN THE RUSSIAN LIE MACHINE JAMS

39. During its renewed invasion of Ukraine, the Kremlin deployed its disinformation ecosystem in parallel with conventional military tactics. In the last two weeks of January 2022, Russian state media published around 1,600 messages about Ukraine. Between February and March of that year, the government's budget for mass media increased by 433% to RUB 17.4 billion, or roughly EUR 215 million (Kowalski, 2022). The Kremlin aimed to break the will of the Ukrainian people and to promote spurious justifications for its illegal war within democratic countries. Yet its disinformation campaign was very far from achieving these objectives.

40. This failure was due to several factors. Firstly, the Russian leadership undermined its own disinformation campaigns by initially denying that it was waging war on Ukraine. As a result, Russian disinformation actors were hesitant to show images of the war and its violence. This **passive stance** left the information space wide open for Ukrainians to successfully denounce the brutality of the Russian armed forces to the world.

41. Secondly, the Kremlin's disinformation campaign was thwarted by several Allies who **pre-emptively countered** the lies that the Kremlin planned to use to justify its invasion of Ukraine. For instance, the US quickly declassified information concerning a fabricated video of false atrocities that the Kremlin intended to release before ordering troops already positioned at the Ukrainian border to invade. By catching the Russian regime off guard, the US administration exposed the Kremlin's deceit to the international community, eliciting a more united and stronger response from democratic countries to the illegal aggression against Ukraine (Barnes and Cooper, 2022).

42. Finally, once confronted with the shock of seeing war return to the European continent, Allies and their democratic partners acted in unison to limit the ability of Russian disinformation actors to manipulate the information space. They implemented unprecedented **sanctions** against Russian organisations and individuals engaged in disinformation activities. The UK, Canada and the European Union (EU) banned the broadcasting of *RT* and *Sputnik*, while *RT*'s US service closed shortly after the invasion began. Although these media outlets remain accessible through back-door channels, such as by using virtual private networks or viewing their websites in countries that have not banned their broadcasting, their reach has been significantly reduced by sanctions. Other actors, including fake civil society organisations and publications linked to the Russian intelligence services, have also been subject to sanctions (Kern, 2022). This swift and effective response by democratic countries prevented Russia from disseminating a deluge of lies about its aggression.

B. THE SUCCESS OF UKRAINIAN ANTI-DISINFORMATION MEASURES

43. The Ukrainian response to the Russian invasion is not confined to the battlefield but has also been effective in the information space. Having faced Russian disinformation campaigns for almost two decades, Ukraine has proven itself far more agile and effective in this area since 24 February 2022 than the Kremlin had anticipated. The country had already taken steps to combat disinformation well before the latest conflict began. Between 2014 and 2022, Ukraine banned several media outlets that were spreading pro-Russian disinformation, launched media literacy initiatives on disinformation, and set up organisations to expose Russian lies (Diepeveen et al., 2022).

44. When Russian troops crossed the border, Ukrainian society was therefore able to respond quickly in this domain. Its approach can be divided into four main areas. Firstly, the Ukrainian government, civil society and media **immediately countered** the false information spread by the Kremlin, particularly regarding the alleged capitulation of the Ukrainian government and the exaggerated extent of its military losses.

45. Secondly, **Ukrainian society as a whole mobilised online**, using multiple languages to condemn the violence and cruelty of Russian attacks against Ukrainian civilians. These efforts received global attention and generated widespread support for Ukraine. The response was all the more effective since nearly 77% of Ukrainians actively use at least one social media platform and almost the entire country had internet access before the invasion (OECD, 2022). As a result, the Russian aggression in Ukraine became the first conflict to be experienced in real time by the entire world on social networks, with the abuses of Russian troops widely exposed online and condemned by the international community and public opinion.

46. Thirdly, **Ukraine was able to humanise its resistance** and thus strengthen the resolve of its people to fight and garner foreign support. While Russia has resorted to outdated and impersonal communication, public opinion abroad has been swayed by Ukrainian images of soldiers getting married on the frontline, farmers towing abandoned Russian armoured vehicles, and displaced persons carrying their pets. Similarly, stories of the heroism of real or imagined Davids fighting a rampaging, bloodthirsty Goliath, such as the defenders of Snake Island, have embodied the resistance of the Ukrainian people and commanded the world's admiration. No hero, however, has been a more effective communicator than the Ukrainian President, Volodymyr Zelenskyy. Through regular and personal videos, he has galvanised the Ukrainian resistance, united citizens behind their democratic authorities and armed forces, and vastly increased international support for his country (Beard, 2022).

47. The fourth and final angle in Kyiv's approach has been to **turn its own information weapons against the Kremlin**. Ukrainian authorities and citizens have used social media to address the Russian population directly, bypassing Putin's disinformation machine. They could thus extol the successes of the Ukrainian armed forces on the battlefield, highlight Russian military failures, and reveal the human and economic cost of the illegal and unjustified war launched by the Kremlin (Adams, 2022).

48. Despite Ukraine's commendable successes in countering the Russian disinformation machinery, it is imperative to offer the country increased support in its battle against this menace. In this regard, Ukraine's proposal to establish an "informational Ramstein" should be seriously considered and implemented by the Allies (Tkachenko, 2022). Modelled after the Ukraine Defense Contact Group that regularly convenes at Ramstein Air Base, such a framework would facilitate the coordination of Ukrainian and Allied strategies for combatting Russian disinformation, and provide more efficient and precise assistance to Kyiv in this critical area.

C. THE ENSUING EVOLUTION OF RUSSIA'S DISINFORMATION STRATEGY

49. Ukraine has surpassed Russia in the information space, an area that the Kremlin believed it could rule. In response, the latter has been forced to adapt and intensify its disinformation campaigns. **At home**, the regime has **further increased efforts to manipulate information** available to the Russian public. The Kremlin is no longer able to deny the war's existence to a population impacted by its ever-growing human and economic costs. It has therefore launched a relentless campaign to legitimise the aggression by framing it as an operation to liberate Russian-speaking populations. The regime has also falsely accused Ukraine of targeting civilians and claimed that Russian forces are gaining the upper hand on the battlefield. Furthermore, reality is being distorted in Russian schools, where teachers were instructed by the Education Ministry to screen a video of President Putin justifying the invasion (Van Esveld, 2022). Similarly, the Ministry of Culture ordered cinemas to project biased documentaries glorifying Russia's war of aggression (Hall and Ivanova, 2023). By creating a parallel world of lies, the Kremlin hopes to retain the support of the Russian population and prepare them for future sacrifices, despite repeated military failures (The Economist, 2022b; Diepeveen et al., 2022).

50. These efforts to manipulate information go hand in hand with **a radical escalation of the Kremlin's already fierce repression** of independent voices in Russia. Shortly after the latest conflict began, the Russian authorities fined and threatened to shut down platforms that described its renewed attack on Ukraine as a "war" or "invasion" (Gessen, 2022b). They also blocked social media sites like Twitter, Facebook and Instagram, and limited access to major Western news sources (The Economist, 2022b; UN News, 2022). In addition, they passed a law that could result in a 15-year prison sentence for spreading "false news about the military" (Reuters, 2022). Considering the risks posed to their journalists by this law, many Western news channels, including the BBC and *France24*, have had to leave the country. The few remaining opposition sources in Russia, such as *TV Rain* and *Radio Echo* in Moscow, were forced to stop broadcasting due to increasing pressure from the Kremlin (Gessen, 2022b). This narrowing of the information space makes it more difficult for Russians to access independent news sources not spreading the regime's lies (Robinson et al., 2022). Moreover, the authorities have arrested over 15,000 people for participating in anti-war protests or for opposition activism (McCarthy, 2022). Among them is Vladimir Kara-Murza, a prominent Russian dissident, who is charged with "high treason" for spreading allegedly false information about the activities of the Russian army in Ukraine, including at the annual session of the NATO Parliamentary Assembly in Lisbon in 2021 (Borogan and Soldatov, 2022). The General Rapporteur has called for his immediate release, along with that of all political prisoners in Russia and Belarus.

51. **Abroad**, the Kremlin relies on **alternative platforms** to circumvent sanctions against its media and continue to spread its lies in Western countries. The messaging application *Telegram* has notably become an alternative network for the spread of Russian disinformation (Fredheim and Stolze, 2022). Furthermore, since February 2022, websites posing as independent think tanks or news organisations have emerged, disseminating false information from Russia (Klepper, 2022). *RT* and *Sputnik* also continue to exist online through new accounts with similar domain names.

52. Russian disinformation actors have also adopted **new methods of dissemination**. For example, since May 2022, a Russian disinformation network has cloned the websites of at least 17 foreign media outlets (including The Guardian, *Der Spiegel*, the Ukrainian media outlet *ORBC, Le Monde, Le Parisien* and *20 Minutes*), and of the French Ministry for Europe and Foreign Affairs, by buying fake domain names and publishing false information (Alaphilippe et al., 2022). This Russian campaign, nicknamed "doppelganger" and targeting important Western media sources and public institutions for over a year, raises concerns about the potential for large-scale public manipulation. Moreover, manipulated videos, articles and tweets professing to be from Western media regularly appear online, spreading Russian disinformation through new channels while discrediting the media outlets concerned (Weber and Baig, 2022).

53. The Kremlin has also intensified its efforts by **expanding its international reach** in the information space to garner international support for its invasion and counter the Western authorities' resolve to prevent the spread of Russian disinformation. After the collapse of the USSR, the Kremlin pursued anti-Western disinformation that glorified Russia to post-Soviet countries and to several non-democratic states aligned with the Soviet Union. In recent years, however, Russia has been building a global disinformation network, targeting new countries in multiple languages. Russian lies have been taking root in parts of the Middle East, Africa and Latin America, where the Kremlin often exploits existing anti-Western sentiment. Since February 2022, this network has become even more significant. For example, between 24 February and 4 April, the number of tweets posted by the Arabic versions of *RT* and *Sputnik* increased by 35% and 80% respectively. Most of these messages relay false or manipulated information about the Russian invasion of Ukraine to fuel pro-Russian and anti-Western sentiment (Janadze, 2022). In Mali, for instance, Russia has been spreading disinformation online since the deployment of its mercenaries in late 2021, with the primary aim of discrediting the French presence and justifying its own (Audinet and Dreyfus, 2022). It is also disseminating false information in similar ways in other countries, including the Central African Republic and Burkina Faso.

54. One of the principal lies put forward by Russian actors in these regions is the alleged responsibility of Western sanctions for global shortages and rising food prices. Russian media is transmitting these messages in several languages, with Chinese counterparts amplifying them and thus expanding their influence in the countries concerned (EUvsDisiNFO, 2022). Russian officials have also picked up on this narrative. For instance, Foreign Minister Sergei Lavrov repeated these false claims during a visit to several African countries in August 2022, and urged their leaders to call for the lifting of Western sanctions (Steinhauser and Bariyo, 2022). Russia is thus deviously using a food crisis of its own making to gain support from the countries most affected by it.

VI- OVERVIEW OF THE MAIN MEASURES USED TO COMBAT RUSSIAN DISINFORMATION

55. National authorities have the primary responsibility of combatting disinformation, and in recent years, individual Allied states have implemented various measures towards this end. These include developing **legal frameworks** for online platforms that improve the removal of disinformation content and the transparency of advertising funding, while also upholding freedom of expression. Some of this legislation aims to protect electoral processes from disinformation, such as the law to combat information manipulation adopted by France in 2018. This law allows a judge to intervene during the three months preceding an election to prevent the spread of false news; it compels social networking companies to disclose the funding source of political advertisements on their platforms; and it empowers the French Regulatory Authority for Audiovisual and Digital Communication (Arcom) to block television and radio stations that are under the control or influence of a foreign state and disseminate disinformation.

56. In addition to these legislative efforts, individual Allies and partner states have established **specific bodies to counter disinformation**. For instance, in 2017, the Czech Republic founded the Centre Against Terrorism and Hybrid Threats, which notably monitors and analyses disinformation campaigns that threaten the country's security. The centre suggests legislative measures to better protect Czech society from this threat and collaborates with civil society on public awareness-raising initiatives.

57. Furthermore, to enhance their citizens' resistance to disinformation, certain Allies and partner states have launched **awareness campaigns** and supported **media literacy programmes**. The UK, for example, created a programme through the Department for Digital, Culture, Media and Sport (led at the time by the current Vice-Chair of our Committee, Dame Caroline Dinenage) that assists

librarians, teachers, youth workers and caregivers in training young people and individuals with disabilities to detect online disinformation more effectively (Government of the United Kingdom, 2021).

58. To raise public awareness and effectively expose Russian lies, Allies have **collaborated with civil society**. Think tanks, research centres and fact-checking organisations have been involved in identifying, denouncing and countering Russian disinformation networks. For instance, the Estonian website *propastop.org* plays a crucial role in exposing malicious Russian narratives and strengthening media literacy (CSIS, 2020).

59. Another vital aspect of countering the spread of Russian disinformation is promoting and disseminating verified and objective information within the Alliance and worldwide. To this end, several member states provide funding and support for **international public service media** such as *Deutsche Welle*, BBC World Service, *France Médias Monde*, and the U.S. Agency for Global Media (Garriaud-Maylam and Vall, 2020). Similarly, the Franco-German channel *Arte* has developed a programme called *Désintox*, dedicated to exposing attempts at manipulation. These media outlets, often broadcasting in multiple languages, actively participate in exposing Kremlin lies, particularly in regions where it has recently stepped up efforts to manipulate information, such as Africa, the Middle East and Latin America.

60. In response to Russia's renewed invasion of Ukraine, national authorities in Allied countries have taken action against individuals and entities involved in spreading the Kremlin's false and manipulative narratives. As previously mentioned, the UK, Canada and the EU have blocked the broadcasting of *RT* and *Sputnik*, and the US version of *RT* has ceased its operations. **Sanctions** have also been imposed against fake civil society organisations and publications linked to Russian intelligence services. For example, in March 2022, the US Treasury Department sanctioned and blocked the US assets of 11 organisations operating under the influence of Russian intelligence services (Kern, 2022). Canada has also imposed sanctions against several individuals and entities disseminating false Russian information (Government of Canada, 2022).

61. Allied national authorities have stepped up pressure on **social media companies** to respond to the threat posed by Russian disinformation in the context of the invasion. In March 2022, Facebook thus announced that it had identified and reduced the visibility of Russian state media posts, in addition to complying with specific measures required by individual Allied countries (Meta, 2022). Twitter, YouTube and other platforms have taken similar steps (Myers and Frenkel, 2022). These efforts greatly reduced the reach of Russian lies on social networks in the aftermath of the invasion (Dwoskin et al., 2022). Yet they seem to have become less effective in the following months, notably due to a lack of investment in new technologies for filtering malicious content and a lack of staff with Russian and Ukrainian language skills (Oremus, 2022). In addition, some social media platforms do not block Russian disinformation, including the Chinese company TikTok. Allied governments must continue cooperating with social media companies to ensure their sustained involvement in the fight against Russian disinformation. Nonetheless, the definition of what constitutes disinformation, which goes beyond freedom of expression, should be determined by elected institutions and not by private companies.

62. The Allies have also taken proactive measures to counter the Kremlin's distortion and manipulation of historical narratives to justify its criminal and unlawful actions. A prime example of this manipulation is the glorification of the Holodomor, a deliberate famine orchestrated by the Soviet regime in 1932-33, resulting in the deaths of millions of people in Ukraine. To combat the Kremlin's historical denialism, several Allied parliaments (including the French Senate through a resolution introduced by the Rapporteur) have adopted texts advocating for the recognition of the Holodomor as a genocide. These endeavours are of utmost importance and should be replicated across all Allied nations. They serve a dual purpose: to honour the memory of the victims, and to send a clear message to Russian leaders and forces currently involved in grave offences in Ukraine, including

potential acts of genocide, that history cannot be rewritten through disinformation. NATO collectively recognises the threat that Russian disinformation poses to security and democracy in Allied countries. The latest **Strategic Concept** of June 2022 acknowledges that authoritarian actors, including Russia, "challenge our interests, values and democratic way of life", notably through disinformation campaigns. Allies also emphasise that "the Russian Federation is the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area", employing "conventional, cyber and hybrid means" against them and their partners (NATO, 2022). In a similar vein, in the Brussels Summit Communiqué of June 2021, Allies had already highlighted that "Russia has [...] intensified its hybrid actions against NATO Allies and partners", including through "widespread disinformation campaigns". They pledged to enhance their capabilities to prevent and respond to this threat, as well as to increase cooperation between NATO and the EU in this domain (NATO, 2021).

63. As NATO is a frequent target of Russian disinformation campaigns, it has taken **active measures** to **counter such false narratives** and disseminate factual and objective information. The NATO Public Diplomacy Division has created a web page titled *NATO-Russia: Setting the record straight*, which debunks myths and falsehoods spread by Russian disinformation about the history of NATO-Russia relations and the Ukrainian conflict. This web page is available in Russian and Ukrainian along with French and English.

64. But NATO does not seek to debunk every Russian lie. Instead, it takes a **proactive, rather than reactive, approach** when communicating the Alliance's objectives and actions, including to the Russian public. NATO follows a three-pronged approach that involves developing an understanding of the information environment, adapting its strategic communication to it, and coordinating its efforts with partners. Until its closure in 2021, NATO had an information office in Moscow. Since then, it has pursued efforts to reach the Russian public by adopting new communication techniques, despite the obstacles created by the regime. These include creating a graphic novel, live-streaming sessions on gaming platforms like Twitch, and inviting influencers and journalists to its headquarters, including Russian journalists.

65. NATO also provides **support and expertise** to member countries to strengthen their resilience to Russian disinformation. It promotes the sharing of best practices among Allies and assists in the development of national strategic communication networks and capabilities. It occasionally deploys Counter Hybrid Support Teams to Allied countries, at their request, to help them prepare for or respond to disinformation campaigns. Such teams were brought together to assist Montenegro in 2019 and North Macedonia in 2020 in combatting Russian disinformation online, particularly in the context of elections (Sanchez, 2021). In addition, NATO has developed a toolbox to assist Allies in assessing and responding to hostile information activities.

66. NATO also serves as a platform for member states and partner countries to **collaborate** on countering disinformation. One example of such cooperation is the NATO-Ukraine Platform on Countering Hybrid Warfare, which was established in 2016 to exchange information on detecting and building resilience to Russian disinformation. NATO likewise works with other relevant international organisations facing the same threat, particularly the EU. In 2016, the EU-NATO Joint Declaration identified the fight against hybrid threats, including disinformation, as an area of cooperation between the two organisations (EU-NATO, 2016). The third Joint Declaration, adopted in 2023, reaffirmed their commitment to working together in this area (NATO, 2023). These declarations have led to regular consultations at the leadership and specialist levels. In parallel to this development in EU-NATO relations, the EU has stepped up efforts to combat Russian information manipulation. In March 2015, it created the Task Force East Stratcom, under the aegis of the European External Action Service, to analyse disinformation trends, refute false and manipulative narratives, and raise public awareness. The EUvsDisiNFO project also exposes disinformation – mainly from Russian sources – and highlights the risks it poses to democracies. In 2018, the EU adopted a Code of Practice on Disinformation, which aims to curb the spread of fake

news online, especially during elections or crises. The main global players in the sector have committed to complying with it. However, it is concerning that in May 2023, Twitter made the decision to withdraw its commitment (Egloff, 2023). This code was further strengthened in 2022, with commitments to increase the transparency of online political advertisements, reduce financial incentives for actors spreading disinformation, and deepen the fight against fake accounts, bots and other techniques used by these actors. Together with the regulation on transparency and targeting of political advertising and the Digital Services Act adopted in 2022, this new code forms a robust regulatory framework that enables EU members to better address the threat of Russian disinformation.

67. Lastly, NATO cooperates with several **centres of excellence** working in the field of disinformation. The European Centre of Excellence for Countering Hybrid Threats, based in Helsinki since 2017, serves as a platform for research and expertise sharing among its member states, the EU and NATO. It also conducts exercises aimed at countering Russian disinformation (Hivert, 2022). The Centre for Strategic Communication Excellence (CSCE), based in Riga since 2014, contributes to enhancing the capabilities of NATO and its member states in the field of strategic communication and the fight against disinformation.

VII- CASE STUDIES

A. FINLAND: EDUCATION AND AWARENESS AS PILLARS OF SOCIETAL RESILIENCE TO DISINFORMATION

68. Finland has consistently topped international rankings for its resilience to disinformation (Lessenski, 2022). Finnish efforts in this area are fully in line with the country's total defence policy (Schultz, 2017). The authorities recognise that preparing for hybrid threats, which include disinformation operations, requires in-depth cooperation between all sectors of society, encompassing the public and private sectos, civil society organisations and citizens themselves.

69. Education is at the heart of Finland's success in combatting disinformation. Since 2013, the Ministry of Education and Culture has been developing multi-year guidelines for media literacy (Finnish Ministry of Education and Culture, 2013). The Finnish education system has thus become an example for other Allied countries to follow in this field. Media education and the detection of disinformation are an integral part of children's school curriculum from an early age (Benke and Spring, 2022).

70. In addition to being dedicated to educating the youth, Finland also prioritises raising awareness about the perils of disinformation within vulnerable segments of society. Notably, workshops tailored for the elderly are conducted in public spaces, imparting essential skills required for recognising disinformation (Gross, 2023). A fact-checking organisation, Faktabaari, also designed a digital toolkit accessible to all citizens during the 2018 elections to heighten awareness and prepare them for potential disinformation campaigns (Faktabaari, 2018).

71. The Finnish approach to combatting disinformation is therefore distinguished by its strong emphasis on education and awareness raising. Alongside its institutional efforts aimed at strengthening content moderation of traditional and online media and debunking false and harmful narratives disseminated by Russia and other actors, Finland is successfully educating its citizens to reject disinformation for themselves. In doing so, it fosters the emergence of a "fact-checking society" in which every member is well-equipped to detect fake news and navigate safely through an increasingly complex information landscape.

B. ROMANIA: INCREASED VIGILANCE AND A WHOLE-OF-GOVERNMENT APPROACH TO COMBATTING RUSSIAN DISINFORMATION

72. Romania has been a recurring target of Russian disinformation operations since its democratic transformation and transatlantic integration. At least 55% of Romanians were exposed to disinformation in 2021 (INSCOP, 2021). Since the start of Russia's new illegal aggression against Ukraine, Russian destabilisation operations using disinformation have increased in number and intensity.

73. During the visit to Romania by the Committee on Democracy and Security in April 2023, Romanian officials explained the significant strides the country's institutions have made in combatting disinformation. The authorities diligently track and analyse Russian disinformation operations even before they take root. Several ministries have set up early warning and detection systems, maintaining a vigilant watch over the information landscape.

74. This constant monitoring enables the various Romanian institutions involved to respond swiftly and effectively when a hostile narrative gains traction online or in traditional media. They respond in collaboration as part of a whole-of-government approach that strengthens their credibility and citizens' trust. To achieve this, they use a wide range of channels to reach as broad a swath of the population as possible. The Ministry of Defence, for example, has created its own anti-disinformation platform, called Inforadar, to expose and rectify false information concerning the country's security and defence policies.

C. GERMANY: A ROBUST AND EFFECTIVE LEGISLATIVE FRAMEWORK TO COMBAT DISINFORMATION ONLINE

75. Germany has enacted strong legislative measures to tackle the scourge of disinformation. The Network Enforcement Act (NetzDG), passed in 2018, mandates that internet platforms promptly remove "manifestly unlawful content" within 24 hours of notification, under penalty of fines reaching up to EUR 50 million (La Cour, 2019). This law also requires social media companies to set up complaint mechanisms and provide biannual reports to government authorities regarding the handling of such complaints (Echikson and Knodt, 2018).

76. In 2020, Germany also adopted new media legislation (Interstate Media Treaty) that extends broadcasting oversight to social networks. This legislation gives media regulators the power to take legal action against online platforms that fail to meet journalistic standards. To curtail the automated amplification of harmful content, this legislation stipulates that content created by virtual bots must be clearly identified as such. In addition, companies are obliged to transparently disclose advertising content and divulge information about its funding sources (Bayer, 2021). The text also promotes the dissemination of quality information by requiring certain online platforms to make the journalistic programmes of public broadcasters readily accessible.

77. These legislative advances play a major role in Germany's response to the escalating threat of disinformation. The robust framework they constitute, complementing European legislation in this area, could serve as a template for other Allied nations to better combat the propagation of disinformation online, while upholding the fundamental principles of freedom of expression and the right to information that underpin Allied societies.

VIII- RECOMMENDATIONS

78. Russian disinformation poses a serious risk to the security, but also the democracy of Allied societies. NATO and its members have already taken significant steps to address this threat. Although Russia's use of information manipulation operations in parallel with its conventional attacks during its latest invasion of Ukraine has not proved very effective, it does underscore the need for further action. This general report therefore offers recommendations to Allied governments and NATO to increase resilience to Russian disinformation.

A. INCREASE THREAT AWARENESS AND PROMOTE MEDIA LITERACY

1. **Monitor Russian disinformation**: Allied governments should intensify their efforts to detect disinformation campaigns and map the networks and intermediaries used by the Kremlin to spread false information. Such increased monitoring should also allow them to analyse and track emerging trends in this field and thus better respond to them.

2. **Increase public trust in official information**: Increasing the resilience of democratic societies faced with Russian disinformation requires more transparency on the part of public institutions in the processing and sharing of official information. This transparency is necessary to maintain a relationship of trust between institutions and the public.

3. **Conduct media literacy and disinformation awareness campaigns**: Allied governments should design and support media literacy campaigns so that populations have the knowledge and tools necessary to detect disinformation, including by building on and replicating existing information verification programmes. Educational systems must fully participate in these efforts by training young generations to identify and reject Russian disinformation. Greater support should also be given to civil society organisations active in this field and independent press organisations. It is imperative for Allies to exchange their best practices in this domain, leveraging the valuable experience gained by some among them. In this regard, the Finnish education system stands as a potential blueprint for other member countries seeking to enhance the preparation of the younger generation in identifying and rejecting misinformation.

B. RESPOND TO RUSSIAN DISINFORMATION IN THE INFORMATION SPACE

1. **Allocate sufficient human and financial resources to the fight against disinformation**: While disinformation is a low-cost weapon for the Kremlin, responding to it requires significant resources. Given the scale of the threat, it is crucial that Allies invest in this area, including by building the capacity of institutions specialised in countering information operations and by increasing support for independent media and relevant civil society organisations. Allies should also provide NATO with more human and financial means to detect and counter Russian disinformation about the Alliance.

2. **Refute Russian lies on a case-by-case basis**: Debunking false and manipulative Russian narratives can significantly reduce their reach and impact on targeted societies. In the future, the Allied strategy for countering Russian disinformation should integrate the approach adopted by intelligence agencies in several Allied countries, who pre-emptively expose lies that the Kremlin is about to disseminate to justify its unacceptable actions. This approach should however be deployed selectively. Similarly, it is often crucial to demonstrate the duplicity – and often absurdity – of Russian disinformation narratives once they have gained a foothold in the media, and especially social media. The merits of a rebuttal must nevertheless be decided on a case-by-case basis to avoid giving the regime's lies increased and counterproductive visibility. In this area too, Allies must foster a dialogue among themselves and with their partners to determine the best strategies for countering the narratives propagated by the Kremlin. The Romanian example mentioned in Chapter VII could potentially be transposed to other Allied countries.

3. **Combat the Kremlin's rewriting and doctoring of history**: Allies must take steps to counter the false historical narratives disseminated by the Russian authorities in the information space. In particular, the rehabilitation of the Stalinist regime and the glorification of its criminal actions by the Kremlin must be unequivocally condemned. All Allied parliaments and governments should thus formally recognise the Holodomor as an act of genocide.

4. **Counter Kremlin disinformation by speaking directly to the Russian people**: Allies must continue to expose the true face of the Kremlin regime and its corrupt and illegal activities and crimes in Ukraine. Russians must be able to have access to reliable information in this regard. Allies should therefore support independent and democratic voices in Russia and create objective information content for the Russian public.

5. **Combat the international spread of Russian disinformation**: Allied governments should work to better understand and counter the progressive entrenchment of Russian disinformation in Africa, the Middle East and Latin America. The situation in Africa, particularly in Mali and the Central African Republic, should be given special attention in this regard. Allies should promote the dissemination of factual and objective information in these regions, including by investing in media literacy training, supporting independent media outlets, and investing in their international and multilingual public service media, such as *France Médias Monde*, *Deutsche Welle*, BBC World Service and the U.S. Agency for Global Media.

C. REINFORCE THE SOCIETAL AND DEMOCRATIC RESILIENCE TO THE THREAT

1. **Strengthen national anti-disinformation legislation**: Allies should establish strict standards to regulate online content and protect against hostile Russian activities in the information space. It is, however, essential to ensure that such legal frameworks do not infringe upon freedom of expression. The German example in this area could serve as a model to develop common legislative guidelines for all Allies.

2. **Establish a Centre for Democratic Resilience within NATO**: Former NATO PA President Gerald E. Connolly, acting as the General Rapporteur of the Political Committee at the time, first put forward the idea of creating such a centre in 2019. He subsequently made it a central priority during his term as President. The current Presidency, recognising the vital importance of anchoring democratic values at the core of NATO's response to contemporary challenges, continues to champion the establishment of this centre. Importantly, the proposal garners extensive support both within the Assembly and among NATO member states. Upon the request of member states, this centre would provide them with technical support, notably to identify their vulnerabilities to Russian information manipulation operations and jointly develop effective responses. The centre would also serve as a platform for sharing resources and exchanging best practices among member states and partner countries.

3. **Defend democratic institutions and processes from malicious Russian operations**: Building democratic resilience must be a central concern in the Allied response to Russian disinformation. Electoral processes need to be better protected against Kremlin interference. This involves various measures: improved cooperation between electoral institutions and the media on strategic communication around elections; increased vigilance on the part of all information actors before and during elections; and a proactive approach to refuting false information by the relevant authorities. In addition, Allied states should rely more often on the support of NATO's Counter Hybrid Support Teams to better protect their electoral processes.

4. **Increase cooperation with social media companies to curb the spread of Russian disinformation online**: Allies must push these companies to be more transparent about the funding of the political advertisements they host and the algorithms they use to recommend content to their users, and to ensure that they do not unwittingly promote Kremlin lies.

NATO governments should also call on these companies to step up the fight against the dissemination of false Russian information on their platforms, especially in languages other than English where moderation is currently inadequate. They should systematically detect and suspend accounts used by Russian actors to spread disinformation.

5. **Test the resilience of Allied societies to Russian disinformation**: Relevant national and NATO civilian and military institutions should conduct regular and thorough assessments of their capacity to respond to Russian disinformation campaigns, in order to identify and address specific and collective potential vulnerabilities.

6. **Block and sanction those who disseminate Russian disinformation**: Since the beginning of the latest invasion of Ukraine, NATO countries have shown strong collective resolve by banning or restricting the dissemination within the Alliance of major Russian media outlets spreading Kremlin disinformation. These measures must be maintained to protect Allied democracies from any attempt at destabilisation in the information space. Allies should also adopt sanctions regimes against individuals and entities playing a key role in the Russian disinformation ecosystem. In particular, the Wagner Group, which helps to spread the Kremlin's disinformation in Russia and abroad, must be sanctioned and recognised as a terrorist organisation by all Allies and their partners.

D. STRENGTHEN COLLABORATION WITH PARTNERS FACING THE SAME DANGER

1. **Continue and increase Allied support for Ukraine to fight Russian disinformation in the context of Russia's renewed invasion of the country**: Allies must maintain their support for Ukraine in the military, humanitarian, political, diplomatic and information fields. As such, they should respond to the Ukrainian request to create an informational Ramstein to better assist Kyiv in this area. They should vigorously denounce the lies spread by the Kremlin in the context of its unlawful invasion of Ukraine. They must bolster their strategic communication with their populations, focusing on the moral and security requirements of supporting Ukraine in its just struggle – not only for independence but also for freedom and democracy. In this regard, Allies need to learn from the Ukrainian response and resilience to the Kremlin's relentless disinformation campaigns during the Russian invasion to develop their own capacity to counter them. Additionally, they should promote the establishment of a special international criminal tribunal to try those responsible for the Russian crime of aggression against Ukraine, including those involved in the dissemination of false information justifying and promoting this crime. Moreover, the criminal nature of what Russian disinformation depicts as humanitarian action has been highlighted by the deportation of children from the occupied territories of Ukraine to Russia and the subsequent arrest warrant issued on 17 March 2023 by the International Criminal Court (ICC) against Vladimir Putin and the Commissioner for Children's Rights Maria Lvova-Belova. Allies must provide their financial and technical support for the ICC's investigation into these abuses.

2. **Strengthen cooperation with democratic countries beyond the Alliance and with multilateral organisations**: Individual Allies and NATO should enhance their exchange of best practices with countries that share their values and likewise face Russian disinformation. Interparliamentary diplomacy, including in the framework of the NATO PA, should contribute to these exchanges. Moreover, the Alliance would benefit from further developing its links with other multilateral organisations working on the subject, notably the EU, to formulate a collective understanding of the threat and agree on common responses and standards.

BIBLIOGRAPHY

Adams, Paul, *How Ukraine is winning the social media war*, BBC News, 16 October 2022.

Alaphilippe, Alexandre; Machado, Gary; Miguel, Raquel; and Poldi, Francesco, *Doppelganger – Media Clones Serving Russian Propaganda*, EU Disinfo Lab, 27 September 2022.

Allan, Duncan; Bohr, Annette; Boulègue, Mathieu; Giles, Keir; Gould-Davies, Nigel; Hanson, Philip; Lough, John; Lutsevych, Orysia; Mallinson, Kate; Marin, Anaïs; Nixey, James; Noble, Ben; Petrov, Nikolai; Schulmann, Ekaterina; Sherr, James; Wolczuk, Kataryna; and Wood, Andrew, *Myths and misconceptions in the debate on Russia*, Chatham House, May 2021.

Audinet, Maxime and Dreyfus, Emmanuel, *La Russie au Mali : une présence bicéphale*, Étude 97, IRSEM, September 2022.

Bandurski, David, *China and Russia are joining forces to spread disinformation*, TechStream, Brookings, 11 March 2022.

Barnes, Julian and Cooper, Helene, *U.S. Battles Putin by Disclosing His Next Possible Moves*, The New York Times, 13 February 2022.

Bayer, Judit, *Policies and measures to counter disinformation in Germany: the power of informational communities*, Heinrich Böll Stiftung Brussels, 13 October 2021.

Beard, Alistair, *The Tweet is Mightier than the Sword: Debunking Disinformation in Ukraine*, RUSI, 7 April 2022.

Becker, Jo and Myers, Steven Lee, *Putin's Friend Profits in Purge of Schoolbooks*, The New York Times, 1 November 2014.

Benke, Erika and Spring, Marianna, *US midterm elections: Does Finland have the answer to fake news?*, BBC News, 12 October 2022.

Borogan, Irina and Soldatov, Andrei, *High Treason, Stalin-Style*, Center for European Policy Analysis, 28 November 2022.

Cray, Kate, *Anne Applebaum: Social Media Made Spreading Disinformation Easy*, The Atlantic, 8 April 2022.

CSIS, *Countering Russian Disinformation*, 23 September 2020.

Denber, Rachel, *The Kremlin's repressive decade*, Human Rights Watch, 13 July 2022.

Diepeveen, Stephanie, Borodyna, Olena and Tindall, Theo, *A war on many fronts: disinformation around the Russia-Ukraine war*, ODI, 11 March 2022.

Dwoskin, Elisabeth; Merill, Jermy; and De Vynck, Gerrit, *Social platforms' bans muffle Russian state media propaganda*, The Washington Post, 16 March 2022.

Dwoskin, Elizabeth, *China is Russia's most powerful weapon for information warfare*, The Washington Post, 8 April 2022.

Echikson, William and Knodt, Olivia, *Germany's NetzDG: A key test for combatting online hate*, CEPS, November 2018.

Egloff, Emmanuel, *Désinformation en ligne : Twitter quitte le code de l'Union européenne, annonce Thierry Breton*, Le Figaro, 27 May 2023.

EU-NATO, *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO*, 2016.

EUvsDisiNFO, *Disinformation fuelling food insecurity*, 26 May 2022.

EUvsDisiNFO, *A Helping Hand: Pro-Kremlin Media Defend China's Human Rights Record in Xinjiang*, 24 May 2021a.

EUvsDisiNFO, *The Least Accurate Oracle in the World*, 16 April 2021b.

Faktabaari, *Fact-checking for educators and future voters: Elections approach, are you ready?*, 2018.

Finnish Ministry of Education and Culture, *Good Media Literacy : National Policy Guidelines 2013–2016*, 2013.

Fredheim, Rolf and Stolze, Martha, Virtual Manipulation Brief, *Russia's Struggle to Circumvent Sanctions and Communicate Its War Against Ukraine*, NATO Strategic Communications Centre of Excellence, January 2022.

Galeotti, Mark, *Active Measures: Russia's Covert Geopolitical Operations*, George C. Marshall European Center for Security Studies, June 2019.
Garriaud-Maylam, Joëlle and Vall, Raymond, *L'audiovisuel extérieur : une arme anti « infox » dans la crise sanitaire mondiale grâce à l'indépendance éditoriale des opérateurs*, Sénat français, May 2020.
Gessen, Masha, *Inside Putin's Propaganda Machine*, The New Yorker, 18 May 2022a.
Gessen, Masha, *The war that Russians do not see*, The Washington Post, 14 March 2022b.
Giles, Keir, *The Next Phase of Russian Information Warfare*, NATO Statcom centre of excellence, 2016a.
Giles, Keir, *Handbook of Russian Information Warfare*, NATO Defense College, 2016b.
Giles, Keir, *Countering Russian Information Operations in the Age of Social Media*, Council on Foreign Relations, 21 November 2017.
Goldstein, Josh and Sastry, Girish, *The Coming Age of AI-Powered Propaganda*, Foreign Affairs, 7 April 2023.
Gordon, Michael, *Russia Copies NATO in War to Win Minds*, The New York Times, 28 November 1999.
Government of the United Kingdom, *Minister launches new strategy to fight online disinformation*, 14 July 2021.
Government of Canada, *Minister Joly announces additional sanctions targeting Russian disinformation and propaganda agents*, 8 July 2022.
Gross, Jenny, *How Finland Is Teaching a Generation to Spot Misinformation*, The New York Times, 10 January 2023.
Hall, Ben and Ivanova, Polina, *Putin shifts war messaging to gird Russians for long fight in Ukraine*, Financial Times, 7 January 2023.
Hivert, Anne-Françoise, *En Finlande, la riposte des démocraties s'organise face aux menaces hybrides*, Le Monde, 4 June 2022.
INSCOP, *Dezinformare, propagandă, ştiri false, încrederea în surse de informaţii*, 31 March 2021.
Janadze, Elene, *The digital Middle East: Another front in Russia's information war*, MEI, 19 April 2022.
Jeangène Vilmer, Jean-Baptiste, *The "Macron Leaks" Operation: A Post-Mortem*, Atlantic Council and IRSEM, June 2019.
Kern, Rebecca, *Treasury sanctions Russian online outlets for spreading disinformation*, Politico, 3 March 2022.
Klepper, David, *Russian disinformation spreading in new ways despite bans*, AP News, 9 August 2022.
Koshiv, Isobel, *Russia accused of trying to use TV to create Ukraine 'digital ghetto'*, The Guardian, 17 February 2023.
Kowalski, Adam, *Disinformation fight goes beyond Ukraine and its allies*, Chatham House, 8 June 2022.
La Cour, Christina, *Governments countering disinformation: the case of Germany*, StopFake.org, 3 October 2019.
Lessenski, Marin, *How It Started, How It is Going: Media Literacy Index 2022*, Open Society Foundation Sofia, Policy Brief 57, October 2022.
Lomas, Natasha, *EU's ban on Russia Today and Sputnik is now in effect*, TechCrunch, 2 March 2022.
Lough, John, *Myth 03: 'Russia was promised that NATO would not enlarge'*, Chatham House, 13 May 2021.
Lucas, Edward and Pomeranzev, Peter, *Winning the Information War*, Center for European Policy Analysis, 2 August 2016.
McCarthy, Lauren, *Why Putin uses Russian law to crack down on dissent*, The Washington Post, 7 April 2022.
McKew, Molly, *The Gerasimov Doctrine*, Politico, September/October 2017.
Meta, *Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine*, 26 February 2022.

Mozur, Paul; Satariano, Adam; Krolik, Aaron; and Aufrichtig, Aliza, *'They Are Watching': Inside Russia's Vast Surveillance State*, The New York Times, 22 September 2022.
Myers, Stenven Lee and Frenkel, Sheera, *How Russian Propaganda Is Reaching Beyond English Speakers*, The New York Times, 9 August 2022.
Nakashima, Ellen, *Inside a Russian disinformation campaign in Ukraine in 2014*, The Washington Post, 25 December 2017.
NATO, *NATO's approach to countering disinformation: a focus on COVID-19*, 13 October 2020.
NATO, *Brussels Summit Communiqué*, 14 June 2021.
NATO, *Strategic Concept*, 2022a.
NATO, *NATO-Russia: Setting the record straight*, 9 March 2023.
NATO, *Countering hybrid threats*, 18 August 2023.
NATO, *Joint Declaration*, 10 January 2023.
NATO Strategic Communications Centre of Excellence, *Analysis of Russia's Information Campaign Against Ukraine*, 2015.
O'Beara, Fearghas, *Russia's war on Ukraine: The Kremlin's use of religion as a foreign policy instrument*, Parlement européen, May 2022.
ODI, *A war on many fronts: disinformation around the Russia-Ukraine war*, 11 March 2022.
OECD, *Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses*, 3 November 2022.
Oremus, Will, *Ukraine says Big Tech has dropped the ball on Russian propaganda*, The Washington Post, 14 July 2022.
Paul, Christopher and Matthews, Miriam, *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Corporation, 2016.
Persson, Gudrun, *Controlling the Past: History and National Security in Russia*, Frivarld, May 2020.
Pynnöniemi, Katri and Rácz, András, *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, The Finnish Institute of International Affairs, 2017.
Reuters, *Russia fights back in information war with jail warning*, 4 March 2022.
Reuters, *Moldova dismisses Russian claims of Ukrainian plot to invade breakaway region*, The Guardian, 24 February 2023.
Richter, Andrei, *La désinformation dans les médias selon le droit russe*, European Audiovisual Observatory, 2019.
Robinson, Adam; Robinson, Olga; and Devlin, Kayleen, *Ukraine war: Russians kept in the dark by internet search*, BBC News, 11 November 2022.
Salvo, David, *Oh, the Irony…Russia Spreads Disinformation about Polish Annexation of Western Ukrainian Regions*, Alliance for Securing Democracy, German Marshall Fund, 5 December 2022.
Sanchez, Linda, *Bolstering the democratic resilience of the alliance against disinformation and propaganda*, Committee on Democracy and Security, NATO Parliamentary Assembly 2021.
Sanger, David, *Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says*, The New York Times, 6 January 2017.
Schultz, Teri, *In defense, Finland prepares for everything*, DW, 10 April 2017.
Snyder, Timothy, *Ukraine Holds the Future: The War Between Democracy and Nihilism*, Foreign Affairs, September/October 2022.
Steinhauser, Gabriele and Bariyo, Nicholas, *Russia Courts African Nations and Aims to Deflect Blame for Food Crisis*, The Wall Street Journal, 25 July 2022.
StopFake, *Manipulation: German Foreign Minister: Ukraine Support More Important than German Voters*, 3 September 2022.
The Economist, *How Russia is trying to win over the global south*, 22 September 2022a.
The Economist, *"There's a real effort to convince viewers that Russia is under attack"—the Kremlin's propaganda*, 20 May 2022b.
The Economist, *The Putin Show: How the war in Ukraine appears to Russians*, 17 May 2022c.
Tkachenko, Oleksandr, *The west must help Ukraine win the information war as well*, Financial Times, 28 September 2022.

Tokariuk, Olga, *A Year of Lies: Russia's Information War Against Ukraine*, Center for European Policy Analysis, 21 February 2023.
Uddin, Rayhan, *Russia, Iran and Saudi Arabia worst countries for state-sponsored Twitter disinformation*, Middle East Eye, 31 March 2022.
UN News, *UN rights experts raise alarm over Russia's 'choking' media clampdown at home*, 11 March 2022.
US State Department *Vladimir Putin's Historical Disinformation*, 6 May 2022a.
US State Department, *Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*, Global Engagement Center, January 2022b.
US State Department, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, 2020.
Van Esveld, Bill, *Russia Instructs Teachers to Spread Disinformation About Ukraine*, Human Rights Watch, 4 March 2022.
Volchek, Dmitry, *Inside The 'Propaganda Kitchen' -- A Former Russian 'Troll Factory' Employee Speaks Out*, Radio Free Europe, 29 January 2021.
Wakabayashi, Daisuke and Confessore, Nicholas, *Russia's Favored Outlet Is an Online News Giant. YouTube Helped*, The New York Times, 23 October 2017.
Watts, Clint, *Russia's Active Measures Architecture: Task and Purpose*, Alliance for Securing Democracy, German Marshall Fund, 22 May 2018.
Weber, Joscha and Baig, Rachel, *Fake content targets international media*, DW, 7 August 2022.