CHAPTER 12

Countering Disinformation: State and International Level

In recent years, many governments have taken more decisive steps to counter the increased spread of disinformation on the internet. In the United States, antitrust proceedings are underway, and proposed legislative changes would hold platforms liable for certain content published on their sites. In the United Kingdom, the regulator requires platforms to protect data and create safer conditions for underage users. The EU has a directive on audiovisual services, and work on a new legal act on digital services has been completed to create further regulations in the Member States and partner countries of the European Economic Area. The COVID-19 pandemic and Russia's invasion of Ukraine have highlighted the need to establish a new, more effective framework for the functioning of the information and internet environment, including social media platforms' efforts to counter disinformation.

1 Dilemmas and the Need to Fight Disinformation

Despite intentions to protect freedom and the right to reliable information, some measures and proposals for combating disinformation face resistance in democratic societies. Facebook's decision to ease its policy on hate speech, however, faced criticism in light of Russia's hostilities in Ukraine. The essence of the social contract lies in finding a balance between security and freedom, and in this paradigm, it is not the state but citizens, civil society, journalists, media, academic and research institutions, and internet platforms that should be on the front line of the fight against disinformation. The Canadian government presented such an approach in 2019 – one that focuses on equipping citizens with the knowledge and measures needed to counteract disinformation (Carvin, 2021). Web regulation does not need to contradict freedom of speech, just as there is no contradiction between driving a car and having a license, using seat belts, or obeying speed limits.

The 2019 report prepared by the OSCE, paradoxically on behalf of Russia, discusses the application of international law and standards that ensure freedom of expression. However, these standards are limited in regard to the rights of other people or the interests of state security, highlighting the tensions

between freedom of expression and restrictions. The issue is not whether restrictions are allowed at all but when and to what extent they are allowed (*International Standards*, 2019). At the same time, calls for a narrow application of restrictions on freedom of expression echoed in UN and OSCE declarations often fall on barren ground in many Member States that subscribe to them, including Russia.

Freedom of expression is enshrined in Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights, and Article 10 of the European Convention on Human Rights. Article 20 of the Covenant prohibits the promotion of war and hate, including based on race. Furthermore, the European Court of Human Rights has ruled that freedom of speech includes offensive or shocking statements, but limitations must be clearly defined by law and must achieve the objectives set out in Article 19 of the Covenant (International Pact, 2021). It is also important to note that false information is considered a violation of the law in various regulatory contexts.

In many countries, penal codes prohibit the dissemination of false information if it causes damage or violates civic, public, or state interests. These prohibitions are usually narrowly defined, however, and sometimes only apply to lies that are disseminated about electoral candidates. Regulations that limit the freedom of expression vary across different countries, with constitutional protections accompanied by statutory solutions and political doctrines. For instance, in Canada, false information that infringes on the public interest is criminalized. Yet even the denial of the Holocaust was not recognized by the Supreme Court of Canada as an unlawful act; it was permitted under the right to freedom of expression.

The Greek penal code provides for up to two years in prison for the dissemination of false information, while the broadcasting law obliges the media to be objective. In Croatia, false market and capital market information are penalized under the criminal code. Kazakhstan has introduced a penalty of two to five years for the dissemination of false information that threatens state security. However, while this activity warrants general analysis, the broad nature of the catalogue of such interests requires special attention. On the one hand, it reflects the changing nature and growing number of challenges to national security, but on the other hand, it may provide a gateway to repressions that authorities interpret loosely as undesirable.

The Lithuanian constitution guarantees the right to freedom of expression, access to information, and information. Nevertheless, it also explicitly states that it does not grant approval for disinformation. This provision has been adopted in the law pertaining to public information access. The

Radio and Television Commission is authorized to penalize broadcasters for instigating hatred or war, but such sanctions require approval from a court. Slovakia has also mandated the obligation of impartiality in its media law, which is overseen by the Media Council. The council has the power to penalize violations, subject to judicial review. In the UK, the media code prohibits false information, particularly in news bulletins aired by broadcasters. Additionally, the UK government communications office sets fundamental standards for content broadcast. However, most of these regulations were established prior to the digital age and the West's current challenge of external disinformation.

To counter new threats, a report by the Brennan Center at New York University's Law School recommends, among others, that a federal commission be established in the United States to define rules for researchers' access to platforms. This would help safeguard users' personal data and prevent illegal targeting (Hendrix, 2021). Such an approach would provide independent and credible social control without requiring the government to take the lead. This does not imply public consent for government inaction, however. In response to the changing nature of disinformation threats, it is necessary to adapt strategies, legislation, and administrative practices. In the West, for example, decisions to limit the activities of the Russian state or Kremlin-supported media were made quickly following the outbreak of full-scale military operations in Ukraine. Estonia and Poland were the first to remove Russian stations from the programs offered by television service providers.

The examples discussed and the data presented below only illustrate a selection of possible systemic or incidental actions and do not reflect the full range of measures taken. Nonetheless, they enable generalizations and conclusions that will be presented further down in this chapter.

- Australia's courts ruled that network publishers are liable for content posted by recipients under their content.
- Canada, Germany, and Poland developed new national cyber defense strategies.
- Estonia revoked the media licenses for *Sputnik*.
- France has implemented legal regulations that impose obligations on platforms. These include storing deleted content and designating employees to contact administration. Additionally, new structures have been established to combat disinformation prior to the 2022 elections. France has also adopted a military doctrine of information operations and identified the Russian perpetrators of the "Macron Leaks" operation.
- German authorities openly accused Russia of conducting cyber-attacks on German politicians.

- Italy opened a national center for combating disinformation.
- Luxembourg refused to grant a television license for the German-language channel *RT*.
- The Netherlands expelled spies and the authorities publicized the attempted hacking attack on the OPCW in connection with the attempt to poison the Skripals.
- Slovakia's internet regulators called for civic organizations and citizens to send drafts of projects to fight disinformation.
- South Korea strengthened public-private partnerships and support for fact-checking.
- Sweden and the United Kingdom created a guide on countering disinformation for officials.
- Switzerland's embassy in Beijing requested the removal of articles on COVID-19 that falsely cited a Swiss scientist.
- The United Kingdom created a law to protect the personal data of minors; it also proposed the appointment of a commissioner for combating disinformation in Scotland.
- The United States has taken several actions, including establishing the State Department Center for Global Commitment for diplomatic measures and sanctions. The U.S. Cyber Command launched a preemptive attack against the Internet Research Agency in St. Petersburg before mid-term elections in 2018. An initiative was also carried out to amend the Internet Act and hold social platforms accountable for disinformation content posted on their platforms. Other legal bills were introduced, including an act on fair advertising and requiring online platforms to give users options to protect their privacy and personal data given that discontent online can lead to violent protests in the streets. Lastly, mandatory media education was introduced in Illinois.

Based on these and other examples, it is possible to catalogue the actions taken relating to countering disinformation both as a general phenomenon and in its international manifestations.

1.1 *Building Structures*

The Viginum unit was established in the Office of the Prime Minister of France with a broad mandate to fight foreign disinformation in the digital domain. The mandate led to the creation of 70 positions in strategy, operational and ethics divisions. In Sweden, the Swedish Civil Contingencies Agency (MSB), entrusted with the fight against disinformation, was transformed in 2022 into the Swedish Psychological Defense Agency, with a broader mandate. In the United States, the Department of State's Center for Global Engagement was

given the competence to cooperate with foreign partners. In Italy, a national hub for the fight against disinformation was created within the European Digital Media Observer network. Its center is the LUISS University in Rome, where fact-checking experts, media experts, researchers, and journalists work side by side. Structural measures of this kind are usually elements of comprehensive solutions that create the premises for a more effective fight against foreign disinformation.

1.2 *Legal Regulations*

In Germany and France, laws were enacted to combat online hate speech and disinformation. These laws served as the foundation for the drafting of the Digital Services Act of the European Union. In the United States, proposals have been put forward for new legislation, including the Fair Advertising Act, which would require platforms to publish and store data on political advertising, including its recipients and sponsors, according to standardized criteria. A proposed bill was also submitted to Congress that would require platforms to provide users with the option to restrict the use of their personal data and block algorithms that control the content they receive (Gold, 2021). Furthermore, the Compulsory Media Education Act was passed in Illinois (Eng, 2021). In Australia, an unprecedented court ruling held publishers accountable for content posted by their audience under their material. Although the effects of states' actions on regulating and combating disinformation are still limited due to the complexity of the issue, individual states and the international community can develop their own solutions.

1.3 *Cybersecurity*

Several countries including Canada, Germany, and Poland have adopted or are in the process of adopting new or revised national cybersecurity strategies. While cybersecurity strategies are important, they cannot replace comprehensive strategies and doctrines to combat the full spectrum of disinformation. An example of offensive preventive actions are the preventative attacks by the U.S. Cyber Command launched against the servers of the Internet Research Agency in St. Petersburg before the 2018 U.S. midterm elections. Other countries, such as Denmark, Estonia, France, and the Netherlands, are also developing offensive cybersecurity capabilities to prevent external disinformation and have offered these capabilities to NATO if needed. The use of such capacities is governed by the existing regulatory framework and international normative framework, as analyzed in the Tallinn Manual series of documents by independent researchers and lawyers. However, the process of intergovernmental agreements within the UN has been unsuccessful for years due to fundamental

differences in the positions of Western countries on the one hand and Russia and China on the other as regards sovereignty over the Internet.

1.4 *Educating Authorities and Officials*

Instructions for these target groups in the form of extensive textbooks were developed in Sweden and Great Britain (Band, 2021). Training programs for public figures, legislative members, and executive authorities are carried out in many countries, including Poland; however, Sweden and Great Britain seem to have the most extensive programs in this regard.

1.5 *Public Warnings*

The United States Department of Homeland Security has implemented a web monitoring system to issue warnings to state and local authorities about potential public order disruptions and violent demonstrations arising from online calls. These warnings are triggered by monitoring the mood and activities of conspiracy groups like QAnon or activities similar to those preceding the events of January 6, 2021 at the Capitol (Sands, 2021). The involvement of foreign agents in inspiring such threats through social media has already been mentioned. To prevent the actions of foreign services, some countries, such as Estonia and Finland, regularly publish intelligence reports on threats, including those related to disinformation and cyber threats.

1.6 *Administrative Decisions*

Prior to Russia's invasion of Ukraine, Estonia revoked the license of the Russian news agency Sputnik. Similar periodic license suspensions were imposed by Latvia and the United Kingdom. Luxembourg denied the German-language channel RT (Lambert, 2021) a television license. In Australia, authorities ordered Facebook to cease the spread of false information on WhatsApp regarding lockdowns and store closures in Sydney during the pandemic (Taylor, 2021). Additionally, Hamburg's Data Protection Commissioner, Johannes Caspar, made decisions limiting Facebook's actions (Schaer, 2021).

1.7 *Diplomatic Actions and Attribution*

Poland reported a cyber-attack on politicians' accounts to the EU and NATO institutions. The Netherlands diplomatically and publicly amplified the attempt and mechanism of a hacker attack on the headquarters of the Organization for the Prohibition of Chemical Weapons in The Hague against the background of the Novichok poisoning of the Skripal family in Salisbury. The Swiss Embassy in China asked the Chinese media to remove deceptive content

in articles it circulated about COVID-19, which incorrectly cited a Swiss scientist (Tewari, 2021). Despite these examples, states rarely take such actions to publicly attribute disinformation or cyber-attacks to the perpetrators.

1.8 *Working Together with the Public*

In Slovakia, the Internet Council has asked societal organizations to send in civic projects to counter disinformation. Long lists of similar examples can be cited, but the ones mentioned above show the spectrum of possible actions at both the national and international level. This leads to the conclusions below.

First, from a global perspective, states are reacting insufficiently and too slowly to the problem of disinformation. Only a few countries (Australia, Finland, France, Germany, Sweden, the United Kingdom, and the United States) have introduced systemic solutions. This applies to countries that are the main targets of disinformation by global state and non-state actors, but also those not in their focus, as in the case of Sweden.

The second conclusion is that, in terms of legal regulations, the most comprehensive solutions have been adopted by France and Germany, with the UK's regulations being less extensive though still significant and precursory. The United States has adopted regulations at the project level, but their adoption remains a significant challenge due to the interests of American technology giants and the political and legal culture. Human rights in the digital age present a difficult dilemma in the fight against disinformation. Proposals by American lawmakers to impose liability for falsehood on platforms such as Facebook are questioned by renowned legal experts who refer to the constitutional protection of freedom of expression.

France and Germany are examples of countries that have enacted strict laws against hate speech, disinformation, and non-transparent political campaigns on social media. This is partly due to experiences with Russia's interference with their state institutions in 2016 and 2017. However, it is also proof of the well-established determination of the societies and authorities in both these countries to counteract disinformation.

Paradoxically, while some democratic countries struggle to find a balance between combatting disinformation and protecting freedom of expression, authoritarian regimes have been using the guise of fighting disinformation to suppress dissent and control the narrative (Dang & Culliford, 2021). Countries such as Russia, China, Pakistan, Belarus, Uganda, and Nigeria have increasingly demanded the deletion of content and blocked internet platforms. Turkey and India are also sometimes leaders in these types of efforts (Paul, 2021). For instance, Uganda blocked internet access after Facebook removed

pro-government accounts, while Nigeria did the same to Twitter over the deletion of a president's tweet. In some countries, disinformation has also been used by the government apparatus and even the military, as seen in South Korea (Tworek & Lee, 2021), Canada, and Jordan (Elliott, 2021a). In the Philippines, the political online disinformation struggle has been characterized as extremely brutal and sexist, while in Afghanistan, the Taliban are using online propaganda to fight their opponents (Pollet, 2021).

A controversial situation also arose when France undertook offensive actions in Africa to counteract Russian disinformation. The French created mechanisms and structures analogous to those in Russia, including a network of false accounts, assuming that they would be able to more effectively limit Moscow's influence over the population of Francophone Africa (Brandt, 2021a). Yet democracies imitating Russia or other active actors in the world of disinformation is counterproductive. It requires submission to authoritarian rules and it legitimizes the disinformation actions of opponents. One may wonder whether Paris, instead of imitating Moscow, should rather appeal to its allies and partners and use political, diplomatic, economic, and cyber tools to increase Russia's costs for such operations. Perhaps a beneficial response would be to initiate a complexity of actions with the EU's participation, including counteracting political corruption and the flow of funds from which influence operations are financed. This in turn would help African states and communities attacked by Russia to create their own instruments for countering disinformation and for supporting free media.

Nevertheless, in France's actions one can recognize and appreciate a strong will to actively oppose foreign influences. Such an approach is also distinguished by the development of military means (including offensive actions) and the adoption of the doctrine of military combat and the fight against disinformation. It seems that, among the countries of the Western community, France, the United States, and the United Kingdom are the most advanced in this aspect of counteracting disinformation.

Based on the research conducted by the authors, a global perspective reveals that only a few countries have made significant efforts to create a comprehensive model for countering disinformation. These countries are:

1. Western countries of global or supra-regional international importance.
2. Countries affected by Russia's disinformation for geopolitical and military reasons, such as Ukraine.
3. Countries with a relatively high income and advanced educational models, which predispose them to quick adjustments. These include the Nordic, and to some extent the Baltic, states.
4. Several states that have taken such steps after experiencing interference with sovereign elections.

It is the task of governments, civil societies, and experts to transform these achievements into a comprehensive, integrated, and sustainable but adaptable system for the entire Western community, encompassing as many countries as possible. Systemic solutions can be distinguished in the countries discussed below (Jeangène, 2021).

1.9 *France*

After the 2017 presidential elections in France, a working group was established consisting of experts from the Ministry of Foreign Affairs and the Ministry of National Defense. The group prepared a 200-page report titled *Information manipulation as a challenge to our democracy* and implemented its recommendations. The report contained 50 recommendations, including that civil society should be on the front line of defense in the adopted model. The report also stated that it was necessary to create administrative structures to detect and counter disinformation, improve the transparency of foreign media registration, and introduce parliamentary hearings on these matters. It also recommended making online platforms responsible for the content they show; strengthening international cooperation within the European Union's East StratCom task force (European External Action Service – EEAS) and the NATO Strategic Communication Center of Excellence in Riga; and intensifying media education and critical thinking curricula for children, teenagers, and adults.

The General Secretariat for National Defense and Security at the Prime Minister's Office and the National Cybersecurity Agency reviewed and analyzed threats, then presented their findings to national stakeholders. Actions were taken in public communication and diplomatic warnings against disinformation were also issued, including at the level of the presidents of France and Russia. In addition, a military doctrine of information operations was adopted, which defines operations of influence using the web as "military activities in the information domain of cyberspace in order to detect, assess, and counterattack, support strategic commands, obtain information or misrepresentation, as a standalone operation or as part of a wider activity" (Kolesnyk, 2021).

Legislators introduced penalties for publishing and disseminating false information in the media, with fines of up to 445,000 euros for intentionally spreading false information that violates public order and up to 135,000 euros for false information that interferes with military discipline, morale, or the nation's war effort. In November 2018, a new regulation was adopted to combat electoral disinformation, which mandated transparency in the dissemination of sponsored information and gave the Radio and Television Council the authority to suspend content from media supervised by foreign countries or related to them, subject to judicial review. The Viginum unit for combating

external interference was established in 2021 as part of the Prime Minister's office, with a budget of around 12 million euros and 70 staff.

1.10 *Canada*

While not the main target of disinformation operations, Canada has taken steps to make the electoral processes more secure. In 2018, a national cybersecurity strategy was adopted and the Cybersecurity Center was established. The Ministry of Democratic Institutions prepared a plan to ensure safe elections, aiming to improve civic resilience and the readiness of political parties. The plan also aimed to counteract disinformation and foreign interference by the administration. A task force for security threats was created, where state information, communication, and diplomatic services cooperate. Additionally, a new legal act on elections was passed to protect candidates against disinformation, ban financing campaigns from outside, and ensure transparency of campaigns, including a register of political advertisements on social media platforms. The government also outlined specific actions they expected from internet platforms.

The Ministry of Foreign Affairs now has a digital policy center with two teams. One team is responsible for the rapid response mechanism and the other for digitizing foreign policy and dealing with the interconnections of digital technologies, moderation on social networks, and issues of artificial intelligence and digital education. Canadian Heritage – country's the Ministry of Culture – is responsible for media education of civil society. The Government of Canada also works together with social media platforms. During the 2018 G7 presidency, Ottawa initiated the establishment of a Rapid Information Exchange Mechanism in the event of disinformation attacks and brought about an agreed framework. It has traditionally supported Ukraine's efforts to combat Russian disinformation, including by providing financial support. In 2020, a citizens' commission was established, and broad public consultations were initiated on regulating the digital market and social media platforms in terms of countering disinformation and hate speech.

1.11 *Germany*

Due to its prominent international position, Germany is a country that faces a high degree of risk and threats relating to disinformation, particularly from Russia. To address these concerns, the Federal Union Treaty on the Media was amended, granting authorities in the union lands the right to initiate proceedings against media disinformation. Additionally, the obligation to mark advertising materials more transparently when using bots was introduced. The role of public service media has also been strengthened, requiring greater

availability of content from such media on other platforms. The German law of 2017 on improving law enforcement online was adopted in response to increased hate speech and disinformation, and it regulates the procedure for complaints about illegal content. This is defined in the criminal code and establishes time limits for removing manifestly illegal content, with removal required within 24 hours or 7 days depending on the nature of the content.

In preparation for the 2021 parliamentary elections, various measures were taken in Germany to combat disinformation. These included public warnings by the spokesperson of the Ministry of Foreign Affairs and publicly attributing disinformation to perpetrators associated with the Russian authorities. Separate websites were set up to provide information about the elections, and the Central Election Commission conducted a dedicated information campaign to promote the transparency of the election process.

Working groups for hybrid threats were established in various state institutions, and knowledge and expertise were integrated into inter-ministerial teams. A team was created at the Ministry of the Interior with representatives from the Ministry of National Defense and the Ministry of Foreign Affairs. The National Cybersecurity Center developed a new cybersecurity strategy that was later adopted by the government. The Federal Office for Information Security conducted training for politicians, decision-makers, and officials and strengthened cooperation with platforms such as Facebook and Google to detect bots and coordinate inauthentic behavior on the web.

Political parties also implemented their own anti-disinformation programs. The Christian Democrats created a fact-checking page, while the Greens established a fire brigade in the *Netfeuerwerk* network. Self-fact-checking initiatives originated in the mass media, such as the DPA-created Fakt21, which focused on training, education, and cooperation among journalistic circles. Similar programs were also launched in the research community of think tanks, including international think tanks.

1.12 *Sweden*

In Sweden, like in Canada and to an extent France, the government's intention is to stay outside the front lines of the fight against disinformation. In this regard, the government in Stockholm has an easier task because Sweden's society is less polarized than in many other Western countries. Furthermore, the opposition thinks similarly to the government in matters of security policy, which creates fewer opportunities for divisions and therefore for external actors to play on them. Swedish society, which also has a high level of general education, is a resilient community largely unaffected by influence operations. In 2018, both the government and civil society, drawing on the experiences of

other countries including the U.S., created a response system. A nationwide media fact-checking platform covering the most important media was established as part of it. Foreign-funded advertising was banned, and relevant teaching materials for pupils and high school students were developed. Based on the experience gained, the Swedish Civil Contingencies Agency (MSB) issued a special guide for public officials and officials dealing with social communication (*Countering Information,* 2019).

MSB, transformed into the Swedish Psychological Defense Agency in 2022, is closely involved with media education in partnership with regions and local authorities as well as social groups and citizens. It cooperates with the private sector, the media, and public relations companies. It also finances research to support subsequent training and education. In addition, it carries out preventive work, including public outreach campaigns.

Sweden works closely with other Nordic countries and the Baltic countries, which look to Sweden for solutions to develop their own prevention systems. The handbook for officials commissioned by the MSB was developed in cooperation with the United Kingdom. Sweden prioritizes the participation of its representatives in international efforts, such as the EU's special task force (EEAS) to combat disinformation and the NATO-affiliated Center of Excellence for Strategic Communication in Riga.

The Swedish system for countering disinformation focuses on key functions, such as coordination, inter-ministerial and international cooperation, education, research, exercises, and strategic communication. Its efforts have proven effective in deterring foreign disinformers.

1.13 *United Kingdom*

London plays a significant role in the international fight against disinformation on account of its experience, global influence and interests, and the worldwide reach of British media and research organizations. British experts have been instrumental in shaping the premises of NATO's communication strategy and are actively involved in its implementation. They have adapted the OASIS (*Objective, Audience, Strategy, Implementation, Scoring*) model of information campaigns for use in NATO, and it is also utilized as a tool to verify the effects of strategic communication efforts carried out by allies. The British have also developed a toolkit for countering disinformation for their public officials, which was developed in partnership with Sweden.

The British approach is also characterized by networking and expertise. There are units in the Office of the Prime Minister and the government chancellery, including teams for communication security, rapid response, and media monitoring. In the Ministry of Foreign Affairs, in addition to the

Russia-focused team, there is an open-source information unit that collects data from research and open intelligence sources. As in Sweden, the British approach distinguishes between two main currents of counteracting: dealing with disinformation in general and targeting specific state disinformers. In connection with the COVID-19 pandemic, a separate interdepartmental coordination team was also created.

1.14 *United States*

The comprehensiveness of the US approach may be debated, but it is showing stronger foundations for countering disinformation in a systematic manner. This was largely spurred by foreign interference in electoral processes, as well as the recent experience of the insurrection on January 6, 2021, when supporters of then-President Donald Trump staged riots at the U.S. Capitol in Washington, resulting in the deaths of six people.

Russia has declared a veritable information war against the United States, the leader of the world's democratic community. The effects of this campaign, as well as American countermeasures, are reflected in official documents, such as the Robert Mueller report on Russia's interference in the 2016 U.S. presidential elections, and numerous reports by research centers, including those of Harvard University, the University of Texas at Austin, and the Massachusetts Institute of Technology. These reports are important sources of conclusions and recommendations for experts, decision-makers, and practitioners in other countries in the Western community.

Despite controversy during Trump's presidency, the United States responded to Russia's disinformation attacks and influence operations with sanctions against the perpetrators. Before the 2018 midterm elections, the American government conducted preventive cyber operations against the Russian troll factory in St. Petersburg. In 2017, as part of a defense package, legislation was passed to counter foreign propaganda. The Departments of State and Defense were mandated to develop a strategy that included assistance to third countries. The Global Engagement Center was established in the Department of State, and it focuses on information technology issues, international cooperation, and the preparation of materials to counter disinformation. The center also works together with U.S. security services.

Senator Amy Klobuchar has introduced a bill in the Senate that would hold companies responsible for allowing misleading information about vaccines and other health issues spread on the internet. The bill proposes to introduce an exception to the current internet law, which has protected companies such as Facebook, Google, and Twitter from legal accusations related to content published on their platforms. The sensitivity of this issue was demonstrated

by limiting liability to current threats to public health, such as epidemics or other situations with mass-scale consequences. The proposed act would not apply when the publication appears organically, such as when it was created by a person rather than an algorithm capable of duplicating it many times (Ghaffary & Heilweil, 2021).

California commissioned RAND to diagnose the disinformation problem during the 2020 elections and make recommendations for the future. The research showed that content prepared by Russian-associated perpetrators was considered by Republican-leaning voters to be a product of the Democratic Party, and vice versa. The materials covered public and social affairs, dividing American voters. One of the researchers recommended that authorities publicly inform the public about the perpetrators and the content of such actions during election campaigns via Public Service Announcements, stating, "Russia knows who does not like whom and what causes divisions, and fills the information space with messages that hinder agreements" (Posard et al., 2021). It is also worth noting instances of local initiatives by the governors of some U.S. states, despite raising controversy. For example, Florida has banned removing candidates' accounts in elections for state and local office, while Texas has banned content moderation by social media platforms, claiming they are supposed to be treated like telephone service providers. Florida's bill has been criticized, however, as an anti-democratic method of tackling undemocratic problems.

1.15 *Poland*

In 2018, Poland was ranked by renowned Czech think tank European Values as one of the countries with a higher awareness of threats related to countering disinformation, mainly among state authorities (Víchová & Janda, 2018). From a broader perspective, however, Poland's weaknesses were identified as the selectivity of actions in cyber-security, dispersion of competences at the administrative levels, and neglect in education and support for independent media.

To counter disinformation, dedicated units have been established in the state administration, including the Ministry of Foreign Affairs and the Ministry of National Defense. The MFA operates the EU Rapid Alert System (RAS) and conducts training in this area, including for the top management of central bodies. The National Security Bureau, the Department of National Security at the Chancellery of the Prime Minister, intelligence and counterintelligence services, the Government Center for Security, and the National Broadcasting Council, which monitors political advertisements, also all deal with issues relating to disinformation. The government administration's activities are

supported by the Scientific and Academic Computer Network (NASK) – the National Research Institute, which answers to the Ministry of Development.

As regards legal issues, Poland's constitution enshrines the freedom of expression in Article 54, while other laws impose certain obligations on the media and specify the conditions for granting broadcasting licenses. The Penal Code defines offenses related to the dissemination of false information. In January 2021, the Ministry of Justice presented a draft law on freedom of speech that deserves special attention due to its potential importance for the information environment in Poland and the fight against disinformation. The drafted law defines the concept of disinformation as false, manipulated, or misleading information that is for profit or with the purpose of violating the public interest. It also refers to the criminal code regarding offenses infringing on personal rights and sets out special obligations for service providers, including semi-annual reporting if they receive more than 100 complaints per year for content posted on their platforms. The draft establishes the Freedom of Speech Council with wide prerogatives to intervene and impose very high financial penalties for misdemeanors. However, the draft does not refer directly to the threats of disinformation by foreign state or non-state perpetrators (Ministry of Justice of the Republic of Poland, 2021).

Commenting on the project, the Polish Ombudsman, in his formal opinion (Public Information Office of the Ombudsman, 2021) opines:

- It is reasonable to remove or block content on social networking sites; however, the draft does not include definitions as to what hate speech is.
- The definition of illegal content did not include the necessary prohibition of discrimination on the grounds of sex, race, ethnic origin, religion, or sexual orientation. The Ombudsman recommended the use of the definition adopted by the Council of Europe.
- It is justified to protect the right to truthful information and the defense against disinformation, content of a criminal nature, or content violating decency, disseminating or praising violence, suffering and humiliation.
- It is difficult to determine the exact number of people who use social media service providers and their portals due to the nature of online communities, the fact that users can choose to be anonymous, and the existence of automated processes.

The Ombudsman also pointed out that the proposed changes to the Electoral Code were questionable and, above all, they pointed to the risk of restricting freedom of speech through arbitrary interventions by the Freedom of Speech Council. This last remark is especially relevant as the method through which members of the council are selected also raises doubts. If it is not possible to select them by a three-fourths majority in Parliament, they may be elected by

a simple majority in the next vote; this stipulation causes concern around its potential to discourage pluralism. The Ombudsman aptly noted that protecting users of internet portals will be more effective within the framework of uniform European standards. It is therefore advisable to postpone the procedure of the project until works in the EU have ended and until the implementation of the Digital Services Act has started.

2 Counteracting Disinformation: a Regional Perspective

Based on the information available, one could consider examining the issue of combating disinformation in Europe from a regional perspective. Northern Europe appears to be the most advanced region in countering disinformation from a political and organizational point of view, and it is characterized by a strong civic, proactive, and integrated approach to the problem. In contrast, the eastern and southern parts of the continent present a mosaic of disjointed, chaotic, or non-existent measures against disinformation. A special case is Ukraine, where after 2014 geopolitics and reality forced the country to deal with unprecedented challenges in the information and cyberspace environment. Additionally, many countries have recently adopted cybersecurity strategies as a response to disinformation threats.

2.1 *Nordic Countries*

The Nordic countries are known for their exemplary resistance to disinformation, including from Russia. Their success can be attributed to their unique societies that are historically shaped by social solidarity, economic strength, high levels of education, and quality media. Finland and Sweden have particularly effective models for countering disinformation, backed by organized education systems that promote critical thinking and creativity at all levels. The Nordic models also employ severe penalties for disinformation. Denmark, for instance, penalizes acts related to media influence and disinformation by foreign states during election campaigns with penalties of up to 12 years imprisonment, although this provision does not cover social media.

2.2 *Baltic States*

Estonia, Latvia and Lithuania are targeted by Russian disinformation due to their geographical location, membership in the EU and NATO, the presence of NATO military forces in their territory, and the existence of significant Russian minorities in Estonia and Latvia. As a result, these countries invest

more in their capacity to counter disinformation and host various analytical institutions, including Centers of Excellence affiliated with NATO: cyber-defense (Estonia), strategic communication (Latvia), and energy security (Lithuania). They have adopted the Nordic countries' solutions to countering disinformation, leveraging their regional proximity and high level of cooperation within the broader EU and NATO framework. Among these three countries, Lithuania is most active in countering disinformation through military means, and it is also the most severely attacked due to its more assertive policy toward countries such as Belarus and Ukraine, which Russia perceives as anti-Russian.

Latvia and Estonia have refused to register branches of Russian state media outlets *RT* and *Sputnik*. However, as they have not yet created an appealing alternative program for Russian-speaking minorities, these minorities still largely remain in the pro-Kremlin information space. In 2017, the Latvian Ministry of Culture launched training programs for journalists in investigative journalism, fact-checking, and media education. Estonia has taken similar actions, introducing compulsory media education in secondary schools. In Lithuania, there is a kind of militarization of the media space, treated by the authorities almost as a separate domain of military operations. Military and civilian experts in psychology, social sciences, cyber security, and intelligence monitor the media, analyze it, and react by reporting incidents that could affect state security. The cooperation between government institutions and society enables Lithuanians to effectively mitigate the impact of disinformation and clean up the information space in a concrete way while protecting decision-making processes. This is a phenomenon of massive societal involvement in the informational security of the state by professional and volunteer teams through projects such as Debunk EU and the Elves movement.

2.3 *Visegrad Countries*

The Visegrad Four countries, namely Czechia, Hungary, Poland, and Slovakia, do not have a homogeneous response to Russian activities and methods of influence, including their perception of threats and responses to them. Their credibility and role of public media also differ. Of the four, Poland is targeted the most by Russia due to historical disputes, regional ambitions, and its role in the EU and NATO. While direct pro-Kremlin disinformation is ignored in Poland, extremely politicized messages are used in public media that exploit phobias, extremisms, conservatism, parochial religiosity, and specific historical examples. These messages deepen social divisions and are conducive to information manipulation by external entities.

In recent years, there has been a stronger desire among authorities in Slovakia to pursue a more proactive information policy. This is taking shape in the form of adopting numerous new documents of a doctrinal or strategic nature. These documents include those on hybrid threats and disinformation, as well as the establishment of new cells in the government's Situation Center and the Government Center for Security Analysis. In 2021, a new security strategy was adopted with provisions on countering disinformation. Additionally, Slovakia's participation in the NATO-sponsored information campaign resulted in a rise in public support for the Alliance in 2020 and 2021 by several points, reaching over 60%.

In Hungary, the close business ties between the political and economic elites and Russia have resulted in Moscow's messaging infiltrating the Hungarian information space through local mainstream media. Furthermore, the media consistently pursues a policy of discrediting the European Union and Western circles. The approach to Russian propaganda and disinformation in Hungary differs significantly from that of other Visegrad Group countries. This divide has been further heightened by disagreements over sanctions against Russia and support for Ukraine after the aggression in February 2022.

Czechia was one of the first countries in the entire EU, and the first in the region, to establish a dedicated unit in the Ministry of Interior and an inter-ministerial structure to counteract disinformation. Taking inspiration from the Baltic states, Czechia employs "elves" who track accounts and online platforms and monitor other related activities, such as campaigns to spread disinformation about COVID-19 (Zamecnik, 2021). The Czech Demagogue has become a source of inspiration for Polish fact-checkers. In 2021, the country adopted a new Strategy for Counteracting Hybrid Threats.

2.4 *Southeast Europe*

In the countries of this region, aside from Ukraine and Romania, the sense of being threatened by foreign disinformation is limited. The COVID-19 pandemic and the related increase in general online disinformation, however, have led to reactions from local governments. Additionally, due to the presence of NATO structures and allied troops on its territory, Romania often experiences Russian disinformation campaigns.

Ukraine is a unique case, in terms of both Russian disinformation campaigns directed against it and its experience and activity in countering them, particularly in the realm of a defensive war following Russia's aggression. In partnership with the European Union and NATO, Ukraine runs many projects aimed at strengthening the media and combating disinformation. The Ukrainian

authorities, particularly since the presidency of Volodymyr Zelensky, have undertaken the daunting task of limiting the presence of pro-Kremlin national media in the Ukrainian information space. This effort included revoking many licenses and blocking access to the most popular Russian-language social networking site, VKontakte. The country has adopted doctrinal and strategic foundations for countering disinformation and established institutions and teams with coordinating functions in the Office of the President of Ukraine, the Security and National Defense Council, and the Ministry of Culture and Information Policy. These teams are actively involved in media education, particularly for schools in eastern Ukraine.

The role of independent Ukrainian media and civil society cannot be overstated, as the supra-regional project called StopFake, including the one existing in Poland, was designed at the Mogilev Academy in Kiev. Civic circles have initiated projects to monitor the image of the state abroad, including one by the Ukrainian diaspora (Havelock & Veliseyeu, 2021). Ukraine has shown that it can effectively defend itself against Russian disinformation during the war and has provided many examples of attempts to reach recipients in Russia itself using popular social channels on Telegram. Ukraine's efforts in combating disinformation undoubtedly provide a uniquely interesting research field, with conclusions that Western countries could use to improve their own tools for combating disinformation.

2.5 *Southwest Europe*

In response to Russia's interference in internal affairs related to Catalonia, Spain has taken the most concrete steps against disinformation among the countries in the region. Its government has adopted relevant action plans and established structures to fight disinformation.

Italy, where the level of pro-Russian sympathies is among the highest in Western Europe and where the political mainstream parties cooperate with partners from Russia, does not seem to be particularly preoccupied with the problem of disinformation, at least at the governmental level. It is, however, the subject of research and prevention of Italian expert and journalistic circles. In 2021, an interdisciplinary national center for countering disinformation was inaugurated at one of the universities in Rome as part of the pan-European EU-supported network, European Digital Monitoring Observatory (EDMO). This network specializes in fact-checking and brings together many organizations from the countries of the region, including Greece, Portugal and Spain. It is unclear, however, whether Russian disinformation is a serious problem on the agenda of the governments of the former two and Cyprus.

2.6 *Benelux*

In the Benelux countries, Russian disinformation is primarily addressed by civil society and the media rather than the government. In 2018, the Belgian government made its first significant attempt to develop a response to disinformation by allocating funds to financially support non-governmental organizations. In the Netherlands, steps have been taken to expose Russian disinformation, including relating to the shooting down of a Malaysian airline plane with Dutch citizens in 2014, as well as an attempted hacking attack on the headquarters of the Organization for the Prohibition of Chemical Weapons in The Hague in 2018. The Dutch organization DROG has had success in counteracting international disinformation through training programs, NATO officer training, and simulation games. The Dutch model emphasizes the credibility of traditional media, which is trusted by the vast majority of society, and public television runs media education projects. Leiden University is a strong center for fact-checking.

2.7 *Global Considerations*

On a global scale, Australia has developed one of the most effective models for countering disinformation. This model, however, has been primarily influenced by the threat of Chinese operations rather than Russian ones. According to the GDI study *Disrupting Disinformation: A Comparative Analysis of Regulatory Frameworks for Countering Disinformation* published in 2021, Australia is the only country that meets the basic systemic criteria for resisting disinformation. This includes combatting hatred, ensuring transparency and effective organization in elections and the functioning of government institutions and task forces, and imposing sanctions on media that violate regulations.

Increased internet control measures are often a response to local tensions and rivalries, as seen in the case of India and Pakistan. In order to limit tragedies such as the scourge of public lynching, often a result of false information circulated on the web, India introduced restrictive regulations. Such disinformation is largely spread through WhatsApp, a particularly popular platform in India.

In Indonesia and Turkey, the authorities' control measures aim less to protect citizens' interests and more to protect the interests of the ruling parties. Even nominally independent fact-checking organizations, as is the case in Turkey, are focused on monitoring the country's image abroad. In Egypt, individuals with over 5,000 followers on their social media accounts are required to register as media organizations.

After studying the analyzed cases of individual countries, three basic models of the approach of state authorities to regulating the internet can be identified. They are:

- The democratic model, focused on the needs of citizens including their protection against internal and external disinformation.
- The authoritarian model, dominated by the interests of the ruling class and, to some extent, by concern for the safety of citizens, like in India and Turkey.
- The dictatorial model, which ignores the needs of citizens and focuses on full control of the internet, such as in China and Russia.

Most experts agree that the optimal approach for states to tackle disinformation is through a holistic, multi-sectoral, and supra-ministerial approach. Some countries have already adopted this approach, but partial solutions are still dominant. Additionally, many countries tend to focus on combating disinformation during election campaigns and elections, whereas effective countermeasures should be continuous. Another issue is also how to combine the fight against disinformation by foreign states and actors with disinformation carried out by national organizations like political parties. For instance, the Swedish institution tasked with countering foreign disinformation cannot act against its own citizens who spread disinformation for domestic reasons. Similar constraints apply in many other democracies. Clear guidelines are therefore needed on how to differentiate between foreign and domestic disinformation, as well as on how to respond when governments themselves engage in disinformation campaigns targeting their own citizens.

Based on the reviewed national and regional approaches, several elements of an overall systemic structure for counteracting disinformation at the national level have emerged. No country has implemented a complete system, however, although Australia, the Nordic countries, France, and Germany are the closest to achieving this. A complete system should be based on doctrine and strategy and take into account the following considerations:

- Using legal instruments and executive acts in halting disinformation.
- Creating specialized units in the administration structure.
- Establishing structures for protecting elections.
- Demonstrating the ability to analyze the information environment, identify threats, and adapt to them while recognizing one's own weaknesses and groups susceptible to disinformation in the dominant narrative.
- Increasing social resilience and strengthening the credibility of public institutions and mass media, media education, digital education, and critical thinking. This can be done together with journalists and the media.
- Participating in active strategic communication.
- Conducting research that will identify training needs, including for policymakers, politicians, and journalists.
- Working at the local level and with social groups.

– Cooperating with media and platforms.
– Engaging in international cooperation.

3 The EU, NATO, and the UN: Combating Disinformation

The European Union has taken the most comprehensive action in supporting member states in the fight against disinformation, both in general and specifically against disinformation originating from Russia. This began with landmark decisions made in 2015 following the illegal annexation of Crimea and Russia's aggression against Ukraine. These decisions led to the establishment of a specialized task force called East Strat-Com within the European External Action Service (EEAS). Many practical projects and steps have been taken as part of the European Action Plan on Democracy, resulting in new experiences and insights. The Code of Conduct for Combating Disinformation (Killeen, 2021b) was agreed upon as the next stage, and lessons from its implementation were considered in the enactment of the Digital Services Act (DSA). The act imposes many legal obligations, both voluntary and involuntary, on large platforms such as Facebook, YouTube, and Twitter. These include an obligation to cooperate with independent researchers and to allow them to access and participate in complaint and appeal procedures regarding content moderation, dispute resolution, and access to platform archives.

At the social level, the regulation provides for consultations with civil society organizations, as well as the introduction of institutions for trusted whistleblowers to report suspected violations. The act also establishes a European Digital Services Council (DSA) and an advisory body of national coordinators responsible for implementing legislation at the national level. The DSA defines the responsibility of service providers, their obligations, and rules for handling complaints, including out-of-court dispute resolution. It imposes additional obligations on very large internet platforms, those whose services are used by at least 45 million recipients per month, to assess systemic risks resulting from their services, indicate measures to reduce these risks, undergo independent audits, and have conditional algorithmic recommendations and additional transparency for advertisements (*The Digital*, 2021).

NATO relies heavily on strategic communication and media operations to analyze and counter disinformation and propaganda directed at the Alliance's values, goals, policies, activities, and operations. Rather than denying already circulated news, NATO believes that preventing disinformation is more effective. The Alliance's approach is therefore preventive in nature, with a focus

on countering opponents' goals through campaigns that support NATO's role and mission in member and partner states' societies. The Alliance's research and analytical activities are supported by the Center of Excellence for Strategic Communications in Riga and the NATO Defense College in Rome.

In its efforts to combat disinformation, the Alliance has the closest cooperation with the European Union, as well as with the United Nations, the G7, and partner countries. During the COVID-19 pandemic, NATO's steps to counter disinformation demonstrated its ability to sustain its operations, continue its missions and activities, and remain prepared despite the pandemic. This helped ensure that the global health crisis did not escalate into an international security crisis (NATO, 2021).

In 2019, NATO developed a structured package of measures to combat disinformation, which was updated the following year to address hostile disinformation related to COVID-19. In 2021, the Alliance created a toolbox with a two-pronged response model: "understand and act" on one prong and "coordinate" on the other. Its purpose is to provide Allies with instruments to assess hostile information activities and disinformation, and to help identify possible courses of action. Experts from the NATO International Secretariat also organize regular briefings on Russian and other disinformation activities in various Alliance committees, including the Civil Emergency Planning Committee. Additionally, in 2022, the Resilience Committee was established with a mandate to counter disinformation.

As part of the anti-hybrid strategy, Rapid Reaction Teams were put at the disposal of Member States with the participation of strategic communication and counter-disinformation experts. In 2020, NATO further adapted its approach to combating disinformation by increasing support for projects aimed at strengthening social resilience to disinformation in member states. Additional funds were directed towards non-governmental and expert organizations for this purpose.

The role and importance of other international organizations and institutions in countering disinformation are limited compared to NATO and the European Union. Nevertheless, the UN system and the Council of Europe aim to encourage member states to step up their efforts to counter disinformation through actions for media education. These organizations, together with the OSCE, have adopted joint declarations on disinformation threats and media freedom. Since 2018, the OECD has been including the results of media education in PISA surveys. In 2022, the organization launched consultations on the draft *Principles of Good Practices of Response in Public Communication to Disinformation* to support member state governments in improving media and

information ecosystems and creating a space for the exchange and dissemination of information that builds social resilience to online and offline false narratives, thus strengthening democracy (*Public consultation*, 2022).

International trade agreements cannot prevent cross-border disinformation, but they can limit its scale. One proposed solution is to create a model for such agreements within the United Nations, specifically the United Nations Commission for the Law on International Trade. This model would define cross-border disinformation and determine how to attribute it to its perpetrators, as well as prohibit companies from producing and spreading disinformation content abroad. These agreements would also impose obligations to introduce such regulations in domestic legislation (Aaronson, 2021).

The United Nations has established an Information and Democracy program, modeled after the UN process of combating climate change and led by the International Observatory on Information and Democracy. States and civic organizations have also signed the associated Partnership for Information and Democracy, and a global Civic Coalition has been established through the website *information.democracy.org* for the same purpose. The UN agenda also includes raising awareness of the damage caused by global disinformation during crisis situations such as the coronavirus pandemic.

4 Recommendations for Strengthening the Activities of International Organizations: from Practice to Strategy

Organizations that bring together democratic states have implemented various measures to protect themselves against disinformation, but their efforts still appear too limited and defensive. Even the North Atlantic Alliance, which has adapted its approach to disinformation by implementing strategic communication and anti-hybrid strategies, has yet to develop a comprehensive strategy for countering disinformation. Given the increasing threats related to disinformation, measures to counter it should be given higher political priority. This is happening in the EU, as evidenced by the political documents and legislative work mentioned above, as well as by assertive public communication at the political level and Member States' positions on Russian actions.

A new strategic concept was adopted at NATO's Madrid summit in July 2022, where countering disinformation was recognized as a critical issue. The summit aimed to encourage member states to make more explicit commitments to combating disinformation and to hold them accountable for fulfilling those commitments. It also noted that NATO could enhance the mandate of existing

groups dedicated to countering disinformation and strategic communication to facilitate coordination among national efforts, encourage information sharing about threats, and promote effective response measures.

The West's coherent response and resilience building both nationally and internationally should focus on: (1) strengthening social resilience to disinformation; (2) extending preventive and offensive activities; and (3) bridging the differences in practical approaches to disinformation in individual Western countries.

We recommend the following measures.

4.1 *Strengthening Resilience*

- Emphasize broader education regarding democratic values, improving electoral standards, and monitoring campaigns in terms of transparency, fairness, and funding.
- Enforce a media policy aimed at strengthening trust in the media, with stronger and better financed support for media independence and standards, investigative journalism, and fact-checking.
- Take assertive actions toward social media providers. After the new Digital Services Act is adopted at the level of the European Union, it is necessary to support its implementation for the Member States at the national level.
- Conduct information campaigns and more active teaching in schools about the organization's security policy in NATO countries.
- The Alliance should make better use of the network of embassies acting as points of contact to counter disinformation about NATO in partner countries.

4.2 *Preventive and Offensive Actions*

Western countries should more proactively raise the costs for disinformers by publicly exposing their activities and imposing sanctions. Specifically, they should:

- Identify Russian propaganda media operating abroad and harmonize the decision-making standards of regulatory authorities regarding this media. They can also standardize the procedures for punishing media entities for disinformation, including through a suspension of their activities.
- Expose disinformation and influence operations, including disavowing them at high levels through government statements and reports from special services. Such reports should be made publicly available in all NATO and EU member states.
- Employ the proactive use of alert systems within the EU, NATO, and G7.

European states should also take bolder decisions on sanctions against the employees of Russian and Belarusian propaganda institutions.

Within the EU and NATO, and perhaps also in cooperation with the OSCE, a model and practice of pre-bunking activities should be developed as part of pre-election missions in the member states of these communities. As a result, assessments should be developed and partially made public regarding pre-election threats, including cyber threats, and related countermeasures.

National plans presented to NATO allies and accounted for in the annual planning cycle should also be considered as measures to anticipate and pre-bunk disinformation.

4.3 *Bridging the Gap in Resistance to Disinformation*

This group of activities should include:

- Assigning groups, or a joint group, existing within the EU and NATO, to coordinate the exchange of information and experience on good practices on countering disinformation.
- Developing a toolkit for countering disinformation while using existing models in places like the United Kingdom and Sweden.
- Supporting special projects for the Balkan states from the EU, NATO, and the U.S. using the existing networks of delegations, representations and embassies, and resources and funds. This could involve creating a separate program aimed at civil society and the media.
- Creating programs to support local initiatives in the EU and NATO partner countries, where necessary and possible.

5 Conclusion

The main aim of the conclusion is to present a range of existing systemic, doctrinal, institutional, and operational elements of countering disinformation, incorporating the governmental, social, and individual levels. In addition to national frameworks, international frameworks are also established. The effectiveness of many activities is challenging to measure, and their efficacy is often confirmed by experience rather than research. Nonetheless, the examples discussed above demonstrate their effectiveness.

In the United States, a comprehensive analysis was conducted in response to the 2016 election interference. The government released information on Russian disinformation and implemented coordinated measures to protect cyberspace resources during subsequent elections. Authorities proactively

communicated about cybersecurity measures. Social media platforms such as Facebook, Twitter, and YouTube marked election-related content as requiring verification and critical evaluation. Accounts that violated their regulations were suspended. The Partnership for Electoral Integrity was established, and a non-partisan coalition of disinformation researchers identified, tracked, and responded to disinformation. Its main goals were: (1) identifying disinformation before it proliferated; (2) sharing clear, accurate messages about detected disinformation activities; and (3) increasing transparency in the information space.

In connection with the parliamentary elections in 2021 in Germany, the authorities decided to take unprecedented public interventions against Russian disinformation. They took unmasking actions, including warnings at the highest level of the state, attributing perpetration to entities related to the Russian authorities. Hybrid threat teams in various state institutions integrated knowledge and inter-ministerial expertise and increased the efficacy of these efforts.

In Moldova, although a lot of work is still ahead, advancements have been made by legislative decisions and the establishment of governmental institutions to counter disinformation. Media education and the activities of non-governmental organizations contributed to the success of a democratic candidate in the presidential election in 2021. This was a sign that disinformation campaigns became less effective when they were fought more forcefully and when voters consumed more information critically and selectively.

Meanwhile, Russia's invasion of Ukraine in February 2022 created a completely new situation in the fight against Russian information manipulation. The war defied the Kremlin's earlier propaganda about its intentions toward Ukraine as people could see on their smartphones, computers, and television screens the brutal destruction and bodies of those killed in Kiev and its suburbs, in Kharkiv, and in Mariupol, the "Ukrainian Aleppo". The criminal terrorist actions taken by Russia against civilians, including women and children, the deaths of thousands, and the exodus of several million Ukrainians, all brutally exposed the cynicism and real plans of Vladimir Putin and the hypocritical state machine behind him. This propagandistic Waterloo (at the time of writing these words, we do not know the outcome of the war yet) may suggest that the pre-war hybrid actions, including disinformation, were not effective against the West. However, this thesis is not yet proven.

As the rules of peace are replaced by the laws of war, the democratic world rallies behind the victim and condemns the aggressor. However, some argue that if the West had taken decisive sanctions against Russia's propaganda and disinformation apparatus earlier, it could have prevented the war altogether.

This would have demonstrated the West's determination and unity, as well as reinforced its societies' resilience against falsehoods, manipulation, and political corruption from Russia. It would also have signaled a different approach toward Russia than in previous years. During the early stages of information warfare, the Russians were highly effective, while the West was caught unprepared.

Though there is no way of knowing if the war could have been prevented, the Western world stood united in defending the victim of such a brutal aggression and in the face of the attack on the foundations of the international order. Victory over disinformation and authoritarianism is difficult to achieve, however. It remains to be seen when and how Russia will emerge from this war in the long term, and in what direction Russian society will go. It is uncertain if this will mark a bloody farewell to imperial ambitions.

On a global scale, China will undoubtedly learn from the lessons of what happened during the war. The conflict exacerbated existing problems and revealed potential effective solutions and procedures. What may have seemed complicated and requiring difficult arrangements for all members of the European Union became simple and immediately implementable in the face of the war in Europe. The "anti-war" information campaign also broke the monopoly of states, traditional media, and specialized non-governmental organizations in combating disinformation in a spectacular way. The activity of ordinary internet users and groups, such as Anonymous, was astonishing as no one suspected their willingness to join the fight against disinformation on such a large scale. The war also highlighted the importance of leadership, exemplified by Ukrainian President Volodymyr Zelensky. It demonstrated the absolute domination of social media in today's information environment, its strength, and its double-sidedness, as exemplified by the channels used by Russian authorities on the Telegram platform.

The sanctions imposed after the onset of the war met with the expected countermeasures by the Russian regime, including blocking access to Western social and traditional media, and the closure of the last independent editorial offices in Russia. The challenge has become less about defending against Russian disinformation in the West and more about reaching the indoctrinated Russian society.

The Russian disinformation wall created by Putin is not impenetrable. Millions of Russians have installed VPNs to bypass censorship, with 6.4 million Russians installing them in the first three weeks of the war from Apple and Google applications, compared to 230,000 in the three weeks prior. They also use Tor technology to create portals and networks and receive tens of millions of pieces of information about the war via text messages, emails, and online

advertisements. Traditional media also play a role in reaching Russian audiences, with newspapers in Nordic countries, Poland, and Germany publishing materials about the war in Russian or Ukrainian. Most Russians are still heavily influenced by the regime's propaganda, however, with the most important disinformation battleground being large cities, primarily Moscow, and younger generations. Putin has closed the last independent media outlets in response to this.

The extraordinary NATO summit on March 24, 2022, meanwhile, decided that the Alliance will continue to oppose Russia's lies about its war in Ukraine and expose fabricated narratives, operations, and provocations. It also resolved to strengthen the resilience of member states' critical infrastructure and societies to Russian influence, including bolstering cyber-defense capabilities and response to disinformation. Additionally, NATO called on China to stop amplifying false narratives from the Kremlin, particularly about the war in Ukraine and NATO (NATO, 2022). Meanwhile, the European Union adopted the Strategic Compass for the future of international security, which addresses foreign influence and manipulation of information (*A Strategic Compass for the EU*, 2022).

Only time will tell how durable the determination of the Alliance, the European Union, and the West will prove to be in the struggle against disinformation in international politics. It already turns out, however, that such a fight does not have to be unrealistic. On the contrary – the free world is well-placed to win, perhaps especially, in circumstances of war.

Summary

1. What is resilience to disinformation?

Resilience to disinformation refers to the capacity to withstand, confront, and effectively address challenges within the information environment at the individual, societal, and governmental levels, including both civil and military domains. It encompasses the ability to recognize and solve problems, evaluate circumstances and reactions, and take appropriate action in response to false, manipulated, or inaccurately presented information that is systematically and persistently disseminated with the intention of causing harm to individuals or groups.

2. Who is responsible for countering disinformation?

Governments, the media, and civil society, as well as individual participants of processes taking place in the information space should all be involved in countering disinformation. Due to the global nature of the phenomenon, some countermeasures must also be international. It is necessary to integrate efforts at every level of counteracting disinformation, and in particular to create media education programs and legal regulations concerning media, freedom of speech, media market and digital services. Active engagement from social groups and professional communities, particularly journalists, academics, and teachers, is also essential in the fight against disinformation.

3. What is media education and what are its goals?

Media education involves developing an understanding, knowledge, and skills that empower citizens to use the media effectively and safely while also thinking critically to make informed judgments, analyze complex situations, and distinguish between opinions and facts. The ultimate goal of media education is to promote media literacy and pro-social and civic behavior. Essential abilities include accessing a variety of sources to find, use, and share information; evaluating and analyzing the quality, truthfulness, and credibility of different viewpoints; creating content and expressing oneself confidently while being aware of the intended audience and purpose; behaving in a socially responsible and ethical manner that aligns with one's own beliefs and the goals of communication; and engaging socially and civically through the media to achieve political self-realization based on democratic values and attitudes.

4. What does preventing the spread of disinformation at the individual level look like?

To effectively counter disinformation, particularly on social media, it is crucial to internalize certain rules of conduct, including verifying the credibility of sources, platforms, internet addresses, and contact details. This involves checking the credibility of the author and their previous publications, posts, and profile history, as well as scrutinizing the integrity of the text to ensure that it does not contradict itself or other sources and that it is not intended as a joke or satire. Checking the publication date and chronology, as well as paying attention to photos or images for signs of manipulation, is also essential. Additionally, information should be cross-checked in other sources, including with experts, and attention should be paid to the titles and the validity of quotes and expert sources cited. It is also beneficial for individuals to participate in media education and fact-checking initiatives.

5. What is the operating model of social media platforms?

The nature of technology and digital space creates particular challenges related to the spread of disinformation and propaganda, particularly on platforms. These platforms combine four key phenomena in the information space: the aggregation of data about users and their behavior; the algorithmic management of data using computer programs with advanced data processing capacity; the anonymity of aggregation, management, and dissemination of information; and the automation of content publication and user interaction.

Data emission, which is a product of users' activity on the internet, allows platform managers to collect information about users, including their political or election preferences, and to adjust paid communications or advertisements, not only for commercial but also political purposes.

6. What is content moderation?

The primary means of eliminating unwanted content on social media platforms is through moderation. Moderation involves managing and administering the behavior of social media users and involves interference, or lack thereof, in the content generated by users on platforms such as Facebook, Instagram, Twitter, and others, while adhering to their terms and conditions. Moderation is carried out through certain rules and guidelines for posting content, which also restrict and prohibit the posting of unacceptable and inappropriate content. It can occur before publication (preventive moderation) or after it; be algorithmic (automatic) or human-driven. Most platforms use mixed models

of moderation. Additionally, moderation may result in a temporary exclusion, such as account suspension, or a permanent exclusion, such as account deletion, from the platform's community.

7. What is the role of researchers and the media in countering disinformation?

Civil society, including research communities, plays a key role in countering disinformation. It is an environment of exerting pressure, especially on governments, to bring about the desired changes. It helps to recognize disinformation and understand its essence. It provides expertise, advice, and a training base for public service employees. It educates users and actors in the information space.

Journalists are on the front lines of the fight against disinformation. Free media, science and education based on truth and freedom are the foundations of democracy. Because of their role in society, journalists should, above all, avoid duplicating disinformation. One of the main weapons in the fight against disinformation is fact-checking, conducted by the media, and its aim is to improve the quality of public debate and to verify the statements of politicians, officials, or other influential people who find their way into the public space. It is also desirable to broadly include the media community in media education programs in schools and local communities.

8. What is the role of state authorities in countering disinformation?

The most effective national solutions for countering disinformation involve active participation from social and professional groups, supported by the state. The optimal approach is a holistic, multi-sectoral, and multi-departmental one, known as the "whole-of-government approach." This system should be based on a doctrine and strategy, taking into account adequate legal instruments and executive acts, the creation of specialized units within the administration, structures to protect elections, and active strategic communication.

The system must be adaptable to changes in the information environment and provide conditions for developing social resilience to disinformation, encouraging cooperation between the government, media, civic organizations, and corporations that control key social media platforms. Governments also have a responsibility to engage in effective international cooperation in the fight against disinformation.

9. What is the role of international organizations in countering disinformation?

Given the diversity and global reach of actors, goals, and methods involved in manipulating content by both domestic and foreign perpetrators, effective

solutions to counter disinformation can only be developed through collaborative efforts at both the national and international levels. Organizations comprising democratic states have introduced many political and practical measures to safeguard their member states, but their nature still appears too defensive. Combating disinformation should therefore be given higher political priority. A coherent Western response, building resilience both nationally and internationally, should focus on: (1) further strengthening social resilience to disinformation; (2) offensive activities as much as defensive ones; and (3) leveling the differences in the systemic and practical approach to disinformation in individual Western countries.

10. What is the Digital Services Act (DSA)?

The DSA is a groundbreaking piece of legislation that will fundamentally change the information environment in the European Union, member states, and partner states. Its impact will be felt on a global scale as well. The legislation imposes a number of legal obligations on online platforms, including mandatory ones, unlike the Code of Conduct for Counteracting Disinformation. These obligations include the requirement to cooperate with independent researchers, allowing them access to participate in complaint and appeal procedures related to content moderation and dispute resolution, as well as access to archives and data concerning portal usage rules.

At the social level, it involves consultations with civil society organizations and the introduction of trusted entities to signal potentially criminal behaviors. The act also establishes a European Digital Services Council and its advisory body of national digital service coordinators responsible for implementing rules at the national level. The DSA defines service providers' responsibilities and obligations, including organizational and reporting requirements, and rules for considering complaints, including out-of-court dispute resolution. It imposes additional obligations on very large internet platforms used by 45 million recipients per month. These obligations include assessments of systemic risks, measures to reduce these risks, independent audits, algorithmic recommendation conditionality, and transparency of advertisements.