Briefing paper

No 4, December 2023

Countering Disinformation

An Evaluation of the Institutional Approach of Governments

Editor
Dr. Rumena Filipova
Chairperson
Institute for Global Analytics

Author
Dr. Christopher Nehring
Senior Fellow
Institute for Global Analytics

Посолство
на Федерална република Германия
София

This publication is supported by the German Federal Foreign Office. The opinions, findings and conclusions stated herein are those of the author and do not necessarily reflect those of the German Federal Foreign Office.

The briefing paper provides a comparative analysis of the most prominent state agencies established to counter disinformation and foreign influence, featuring examples from the US, the EU, Germany, France, Sweden, Ukraine, Taiwan. The analysis evaluates the institutional approach of these agencies by examining their design and set-up, available resources, main focus of activities, methodological orientation, and communication strategies (horizonal distribution of expertise among government structures and/or vertical public outreach). The advantages of anti-disinformation agencies include increased public awareness, dedication of state resources to fighting disinformation, tracking and assessing disinformation that can affect national security, and intra-government cooperation. However, some pitfalls should be guarded against, including a lack of sufficient information-sharing with the intelligence services and an overfocus on communication of disinformation threats within government rather than consistently reaching out to the wider public, too.

In the face of the renewed urgency and significance of government action for combating disinformation, the main aim of the present study is to provide background knowledge and orientation to the public and policy-makers. The review of counter-disinformation agencies complements our conceptual and institutional blueprint for the establishment of effective strategic communications (as indeed there is a close link between the appropriate remits of strat com and countering disinformation).[1]

The US: Best Practices for Countering Disinformation During and After the Cold War

State-centered approaches to tackling disinformation rose to prominence already during the Cold War. One notable example was the Active Measures Working Group (AMWG) created by the US Government in 1981 to coordinate efforts to detect, analyze, reveal, and debunk Soviet disinformation.[2] The AMWG had access to classified intelligence reporting from the intelligence community. Thus, its methods and focus were influenced by an *orientation* to and partly *reliance* on *intelligence/security work*. The main publications of the AMWG encompassed analytical papers ("Foreign Affairs Notes"), which were distributed domestically and abroad, as well as three extensive, in-depth analyses of Soviet disinformation and "active measures" (the Soviet term for covert influence operations) published between 1986 and 1989. The AMWG employed a *public diplomacy approach*. Especially during the second half of the 1980s the group used public disclosure ("public shaming") as a tool to debunk and counter Soviet disinformation. This public diplomacy approach saw an increased engagement in public communication with the media, journalists, non-state actors and the broad public ("vertical communication"), done via special public press briefings inside the US and abroad, particularly in Europe, to which media, journalists, NGOs, think tanks and others were invited.

Hence, the Active Measures Working Group may be best characterized as an outlet for expert knowledge on disinformation that was *distributed horizontally among state institutions and vertically via public information/ media campaigns*. In terms of design, aims, and methods, the AMWG followed a *security policy approach.* Its most important goal – actively countering Soviet disinformation, however, was reached by means of *public diplomacy*. According to some former members, the strengths of the AMWG and its work included:

- Raising awareness of Soviet disinformation within the US Government;
- Exchanging expert knowledge;
- Sharing access to classified information on Soviet active measures within the US Government;
- Taking an active and confrontational approach to disinformation via public debunking and shaming.[3]

Despite its success, the AMWG's scope of work following the end of the Cold War could not be continued in the same form in the post-1989/1991 period, given the agency's singular focus on Soviet disinformation. Nevertheless, the institutional lessons learnt have informed the background of current US anti-disinformation work, primarily embodied by the *Global Engagement Center* (GEC). The GEC traces its origins to 2011, when the Center for Strategic Counterterrorism Communications (CSCC) was founded within the US State Department for the purpose of "supporting agencies in Government-wide public communications activities targeted against violent extremism and terrorist organizations."[4] Since 2017, the GEC was explicitly given the authority to address other foreign state and non-state propaganda and disinformation activities. In its regional and thematic focus, the Global Engagement Center focuses on disinformation and propaganda campaigns by state actors (particularly Russia, the People's Republic of China and Iran) and non-state terrorist actors.

The GEC is thus the main agency of the US Government in charge of coordinating the fight against disinformation and its mission is to "*direct, lead, synchronize, integrate, and coordinate US Federal Government efforts to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations.*"[5] To fulfil this mission, the GEC has stressed that it uses data analysis as a major tool to analyze and proactively address foreign disinformation and influence attempts. The GEC also shares these (open source) tools, a specially designed information sharing platform as well as training measures with its international partners. The Global Engagement Center has held joint Tech Challenges together with international partners (e.g. Taiwan, UK and Czech Republic), established a full-time liaison to the IT industry at the Silicon Valley, and launched an online repository for information about anti-disinformation technologies (www.disinfocloud.com), which is used by over 335 government users in more than 30 countries.

All in all, the GEC's engagement in the sphere of data analysis, information sharing and IT development is rather impressive, denoting a strong preference for data-based approaches to fighting disinformation. The focus and task of the GEC encompass horizontal communications and information activities within the government and international partners, following a whole-of-government approach.

Germany:
Working Groups and Public Diplomacy

Interagency working groups that distribute expert knowledge about disinformation have also represented the preferred approach for government activities against disinformation in Germany. As declassified documents from the 1980s show, both the German domestic intelligence service (*Bundesamt für Verfassungsschutz* – BfV) and foreign intelligence service (*Bundesnachrichtendienst* – BND) tasked subdivisions of their counterintelligence departments to investigate and analyze Soviet and East German disinformation.[6] Their methods have focused on monitoring and analysis rather than on (support for) debunking or any other countermeasures. The expert knowledge produced here was exclusively distributed in secret to the government itself and other government agencies. Hence, the aim of these groups was to raise awareness among officials and politicians and to inform them about ongoing campaigns. No government agency, neither the intelligence services themselves, nor the Chancellery, the Foreign Ministry, the Army or any other state agency published this expert knowledge or used it for public awareness-raising. Thus, these efforts were characterized by a *security policy approach* and were marked by *horizontal communication and horizontal distribution of expert knowledge*.

The practice of the interagency working group was revived by the government in 2017/18, when the Hybrid Working Group (*Arbeitsgruppe Hybrid*) was founded. It consists of members of the Chancellery, the Foreign Ministry, the Ministry of the Interior, domestic and foreign intelligence and the government's press office who meet weekly at facilities at the Ministry of the Interior.[7] Again, this working group is an informal network and platform that brings government experts together to engage in information exchange about hybrid threats and disinformation. Hence, the group also engages *in horizontal communication and information exchange only*, does not distribute knowledge to the public and *does not engage in actual countermeasures* against disinformation.

Unlike during the 1980s, however, the German Foreign Ministry has additionally established a *unit engaged in efforts to counter foreign disinformation* which is sometimes called "strategic communications" or "public diplomacy", whose 14 employees are headed by the former diplomat Peter Ptassek.[8] This unit is tasked with analyzing foreign disinformation and its impact on German foreign policy, but also devises *measures of strategic communications, public information campaigns, statements and communication strategies*. Contrary to the sphere of activity of most interagency working groups, the German Foreign Ministry is characterized by a *public diplomacy, pre-bunking and proactive communication approach rather than a security policy orientation*.[9]

France:
A Focus on Safeguarding Election Integrity

After Russian attempts to influence the 2017 presidential election in France through Moscow's oft-applied strategy of hacking and leaking, the French government publicly declared the intention to establish an entity within the government to counter similar approaches in the future. The VIGINUM counter-disinformation agency was formally established in the summer of 2021 as a subordinated structure to the French National Security and Defense Council (SGDSN).[10] Although SGDSN's director, Stephane Bouillon, stressed in a public hearing in the French parliament that VIGINUM will not be an intelligence agency, its subordination and the still prevailing secrecy around the agency suggest that the basic design of this unit is marked by a security policy orientation. According to public statements, VIGINUM will eventually consist of a staff of approximately 60 officials,[11] a budget of approximately 12 million Euro[12] and its main remit includes being "responsible for vigilance and protection against foreign digital interference (…), for detecting and analyzing digital campaigns, information manipulation campaigns involving foreign actors and aimed at harming France and its fundamental interests".[13] The focus of VIGINUM's work encompasses *monitoring, detecting and analyzing the tactics, practices, narratives and actors behind digital disinformation and propaganda campaigns*, particularly during the 2022 presidential election, but also regarding the war in Ukraine and French military engagement in Africa.

For the time being, it remains unknown whether VIGINUM will engage in public information campaigns and vertical communication as a single annual report for 2022 is one of its few public appearances.[14] Another, more visible appearance of VIGINUM took place during spring 2023 when the agency helped to uncover a coordinated Russian disinformation campaign. In this incident, French media outlets such as Le Figaro, Le Monde or 20 Minutes were copied by hackers and fake articles about the Russian war against Ukraine were published and amplified online.[15] The ability to expose the malign activity demonstrates VIGINUM's cybersecurity approach to countering disinformation.

All in all, VIGINUM can be characterized as relatively new, comparatively secretive and *small to medium-sized agency* guided by a *security policy approach* towards countering disinformation, focusing on *digital campaigns* and engaging in *horizontal distribution of expert knowledge*.

Sweden:
Empowering a Whole-of-Society Orientation

The Swedish government established an anti-disinformation agency, which officially started its work on January 1, 2022. The Psychological Defence Agency (*Myndigheten för psykologiskt försvar*, MPF) was first subordinated to the Swedish Ministry of Justice and transferred to the Ministry of Defence in late 2022. The main reason leading to the establishment of MPF were expectations of increased Russian influence in the face of parliamentary elections in 2022.[16]

The key tasks of the Agency are to "*identify, analyze, prevent, and counter foreign malign information influence activities and other types of disinformation directed at Sweden or at Swedish interests* (…) *including attempts from foreign actors to weaken national resilience and the population's will to defend the country, or malign influence aimed at changing people's perceptions or influencing behaviours and the decision-making*".[17] Distributing expert knowledge within the administration and government via briefings and reports and building resilience against disinformation within the country inform the scope of the work conducted by MPF. To this end, it functions both preventively and operationally and fulfils its tasks both in peacetime and in the event of war. The Agency describes its approach to countering foreign disinformation as a whole-of-society approach where agencies, municipalities, organizations and not least – the individual citizens, work together. This approach thus includes horizontal communication and distribution of knowledge among government and state institutions, as well as vertical communication via public outreach activities and public information campaigns.

Organizationally, MPF's Operational Department is in charge of threat assessment and the analysis of ongoing foreign influence activities, while the Capability Development Department is in charge of "*providing support to the Swedish population, government agencies, municipalities, the media, voluntary defence organisations, and civil society in general, as well as enabling increased coordination between these actors. Other key tasks include training, exercises and knowledge development, for example initiating and funding research related to psychological defence*".[18] To this end, MPF has produced handbooks for journalists and communicators on how to react to information pressure. Interacting with civil society, particularly with academics, to keep up with and develop new methods to counter foreign disinformation represents a unique feature of the Swedish anti-disinformation agency.

Overall, given the scarcity of available public information, it remains unclear how much of MPF's work is based on a security policy approach; its structure and self-declared profile suggest a strong orientation towards research and public diplomacy. Moreover, unlike many other anti-disinformation agencies, MPF has a *strong domestic orientation* in terms of tackling propaganda. Hence, Sweden's public diplomacy efforts take into account domestic cultural factors and mirror expectations by Swedish society, such as a high level of participation in the political process, public communication and a bottom-up rather than top-down approach.[19]

MPF's work came into view in early 2023, when Swedish and Danish right-wing extremists gathered to publicly burn a printed edition of the Quran. This led not only to a massive foreign policy showdown with many Muslim countries, but also to a wave of digital disinformation and, most importantly, to a diplomatic standoff with Turkey entailing a Turkish veto against Sweden's NATO accession. During this crisis, MPF informed the government about ongoing debates in the digital space and online and offline disinformation and influence campaigns conducted by foreign state actors as well as about close ties between some of the organizers and the Kremlin. These results were further officially presented during a government press conference.[20] As provocative actions such as Quran burnings in conjunction with organized demonstrations continued throughout 2023, MPF persisted in its work in a similar fashion: through monitoring malign informational campaigns, distribution of expert knowledge and advising the government, making public appearances and crafting debunking initiatives.

Ukraine:
Strat Com on the Battleground

In March 2021, Ukrainian President Volodymyr Zelensky established the Center for Countering Disinformationunder the country's National Security and Defense Council. Despite being founded roughly one year before the full-scale illegal Russian invasion of Ukraine, this institutional upgrade of Ukraine's counter disinformation efforts has been overshadowed by Russian aggression towards the country. At the very foundation of CCD lies therefore a wartime and military-oriented mindset, design and framework to counter *Russian influence*.

Despite the focus on disinformation in the agency's name, its tasks and work areas list countering disinformation and propaganda as only one responsibility, while ensuring "information security" and "the national security and national interests of Ukraine in the information space" represent primary objectives.[21] Moreover, CCD reviews and consults international best practice examples for countering disinformation, thus being oriented on international cooperation and attracting international technical assistance. As CCD's updates on international events and cooperation show, their partners have so far included Sweden's MPF, NATO, the EU, USAID, US Civilian Research and Development Foundation.

The Center's public output is well-documented and features training and educational exercises, e.g. for representatives of the Regional Military Administration and the Regional State Administration,[22] the High School for Public Governance,[23] representatives of the central executive bodies and law enforcement agencies,[24] the Agency for Food Safety and Consumer Protection,[25] the State Enterprise National Nuclear Energy Generating Company Energoatom.[26]

Other CCD outputs encompass public debunking ("refutations") of disinformation, a 50-page manual on "How to Counter Disinformation" as well as in-depth analytical reports and shorter articles[27] and conferences. Even though the Center highlights its international outreach and cooperation, its main focus is trained on the domestic audience. There are many more published reports, articles and refutations in Ukrainian than there are in English and significantly more events and training activities in the country involving domestic participants. This might also explain why on the international (media) level, CCD is less visible than other Ukrainian actors employing strategic communications (e.g. the President's Office, Foreign Ministry, Intelligence Services etc.).

Overall, the Center's aims and institutional design are distinguished by several notable features: a *state-centered, security policy and military approach*, with Ukrainian state institutions and the Ukrainian population as its main target groups. The balance between horizontal and vertical communication is difficult to assess as there is little to none information regarding CCD's information exchange and activities on the horizontal, intra-governmental level. This again reflects the *wartime mindset, design and framework* as main characteristics of the Ukrainian counter-disinformation agency. These conditions were also reflected in some controversial measures that CCD took such as the publication of lists of persons accused of promoting propaganda. Among those featured prominent international experts such as journalist Glenn Greenwald or Realist scholar John Mearsheimer. The publication of the list received international criticism charging that such a publication represents a form of public shaming and was, as a result, later deleted.[28]

Taiwan:
Crafting a Coordinated Response

Taiwan is often reported to be the country targeted with the most substantial amount of disinformation in the world.[29] Since 2018, political events such as alleged election interference, press reports and digital campaigns against individuals have led to an increase in government activity vis-à-vis disinformation in Taiwan. In general, Taiwan follows a whole-of-society approach to countering disinformation with numerous civil society, educational and media initiatives operating in this field.[30]

One element of such a holistic approach was the establishment of a government unit to combat disinformation. The Disinformation Coordination Team (DCT) can be described as an intra-governmental working group and comprises officials from the Ministry of Justice, the Ministry of Education, the Ministry of the Interior, the National Communications Commission, and the Central Election Commission.[31] Interestingly enough, DCT is the only anti-disinformation institution known to have engaged not only in extensive exchange and gathering of best practice examples from all around the world (e.g. from UNESCO and the EU), but also in taking considerable time to draft a definition of disinformation on which all participating agencies and officials could agree.[32] DCT's self-declared mission includes drafting policies, interacting with major platforms, and leading interagency discussions. Thus, DCT's organizational structure resembles other interagency anti-disinformation units whose work mainly consists of horizontal communication and cooperation with government bodies and agencies, but is mixed with elements of public diplomacy and vertical communication with the public (see below). As DCT explains, its efforts to counter disinformation are guided by a framework of four elements[33]:

- *Identification*: activities to advocate media literacy to empower citizens to recognize propaganda, mis- and disinformation.
- *Debunking*: provision of guidelines, frameworks, patterns, best practice examples, support and cross-checking for government agencies to refute and debunk false and misleading information.[34]
- *Combating disinformation*: (mostly legal and regulatory) efforts to contain the spread of online disinformation.
- *Punishment*: legal investigations by prosecution and law enforcement to identify and punish the authors and origin of disinformation.

DCT's focus on strengthening public debunking of disinformation has yielded positive results. Yet, efforts to advise, draft and enforce legal and other regulatory measures for containing or decreasing the distribution of online disinformation and for punishing its authors/distributors have been less successful.[35] Despite DCT's aim to cooperate with social media platforms, for example, to ban a pro-Chinese TV station or to stipulate new legislation and provisions prescribing penalties for disseminating disinformation, the distribution of disinformation did not decrease and nor did prosecutors and courts make use of the new legal provisions promoted by DCT.

It has been noted that an ostensible and significant feature of Taiwan's DCT is that civil society and other non-state actors, including journalists and the media, do not engage in close cooperation with the agency out of fear and mistrust of state actors, instead keeping a distinct distance from state-sponsored anti-disinformation activities.[36] This limits the possibilities and incentives of vertical communication, public diplomacy and other public outreach measures of DCT. If DCT engages in vertical communication with the public, it does so via interviews, public statements, debunking of disinformation by state actors and some online publications about the government's efforts to counter disinformation. Nevertheless, Taiwan's whole-of-society orientation for countering disinformation has often been branded as a global best practice model.[37] It needs to be stressed that DCT is only one of many pillars that constitute the country's efforts and activities with media literacy programs, public awareness and non-governmental and journalistic fact-checking and debunking initiatives contributing to the fight against disinformation.[38] Hence, as one analyst remarked, "the framework for countering disinformation created by the Disinformation Coordination Team allows for a swift, coordinated response" while "*civil society and the government operate in mutually enabling parallels. Taiwan's government has become more aware of the harm of disinformation, and high-profile cases increased awareness in society, creating the conditions to make intervention possible*."[39]

The EU:
A Supranational Strat Com Effort

In 2015, as a reaction to the Russian annexation of Crimea, the European Union created its East StratCom Task Force – a unit within the European External Action Service focused on countering disinformation and misinformation. Its main regional focus is the eastern neighborhood of the EU, mainly Russia, Ukraine, Belarus, and Moldova.[40] Yet, over time, the Task Force also started to engage with Chinese influence in Europe and promote European values and narratives in the Maghreb and some countries of the Middle East. These regional specializations are mirrored in its organizational structure, which consists of one task force for each of the three aforementioned regions (East Stratcom Task Force, the Western Balkans Task Force and Task Force South). Besides engaging with foreign information manipulation and interference (FIMI), these three Task Forces develop strategic communications and public diplomacy efforts.[41]

The team of the Task Force was reported to consist of 11 employees in 2018[42] and 16 in 2021,[43] recruited from within the EEAS and other EU institutions. According to its website, the budget of the Task Force was €1.1 million in 2018, €3 million in 2019, €4 million in 2020 and then increased during the Covid-19 pandemic to €11.1 million in 2021.[44] Both staff and the overall budget have been subject to further increases since then.

The self-declared objective of the Task Force is "to gain a more comprehensive, up-to-date and in-depth picture of foreign disinformation campaigns, to reach out with awareness campaigns to new audiences and to increase the EU's and its neighbors' resilience to disinformation".[45] In analyses of disinformation and debunking campaigns, the Task Force focuses on fact-checking messages coming from Russian state-controlled and financed media in EU member state and Eastern Partnership country languages and in Arabic.[46] In doing so, the Task Force focuses on debunking false content and narratives, not on analyzing or blaming the actors behind disinformation. However, particularly since the start of the Kremlin's aggression against Ukraine, some of the articles produced by the Task Force's main outlet "euvsdisinfo.eu", known for its use of satire, puns and "memefication", have used rather sharp language.

Over the past years, the outreach and visibility of the Task Force has increased significantly. Its main tools for communication with the public include the website "euvsdisinfo.eu" and the newsletter "Weekly Disinformation Review", the contents of which are shared via social media such as Facebook and X. According to the Task Force, "euvsdisinfo.eu" had over 1.25 million visitors and 2.4 million page views in 2020.[47] The website also contains a database with the entire collection of disinformation case studies of the Task Force, which comprised approximately 15 000 cases in early 2023.[48] Besides this outlet, the Task Force is very active in organizing events, workshops and giving public talks. *Outreach, public diplomacy and vertical communications measures are thus a strong feature of the Task Force's design*.

On the contrary, little is publicly known about the Task Force's horizontal communication measures within the EU administration and in relations with member states. The Task Force itself points to the EU's Rapid Alert System on Disinformation (RAS) as one major tool and platform for information exchange and best practice transfer with member states and international partners.[49] In addition, the Task Force claims to work with a wide range of partners within and outside the EU administration to share best practices in the field of strategic communications, to ensure support for independent media in the region and counter disinformation.[50] Nevertheless, the Task Force's *focus lies in vertical communications activities* with the public and non-governmental actors. Compared to other anti-disinformation units, the EU's Task Force has no ostensible intelligence- or security policy orientation, but a distinct public diplomacy approach. Its staff and budget are, on the other hand, considerably smaller than other anti-disinformation agencies but its visibility among European media, journalists and the public still increased significantly over the years.[51]

Counter-Disinformation Agencies: Consolidating Strengths and Addressing Weaknesses

The comparative analysis of the anti-disinformation state agencies under investigation reveals a diverse picture, characterized by two major trends. First, *most states have so far preferred to establish small interagency bodies.* Despite increased public attention and the urgency of tackling propaganda, these interagency units usually have comparatively small resources as regards dedicated budget and staff. Nonetheless, as the experience of the US Active Measures Working Group and the EU's East StratCom Task Force demonstrates, even limited resources can be used successfully to fight disinformation – if the agency is backed up by political will and support and if operational work is carried out by committed and motivated employees.

Second, some agencies, such as Taiwan's DCT or Sweden's MPF, privilege a domestic focus on combatting disinformation (i.e. analyzing influence campaigns conducted against local targets), while most others are subordinated to foreign ministries and deal with foreign-originating informational campaigns against a country's international positions and security. Those *agencies with a strong domestic emphasis usually engage more heavily in vertical communications with the public and resilience building*, while *units tackling foreign influence prioritize horizontal communication* based on the distribution of expert knowledge and coordination within the government and administration.

The present study clearly shows that the institutional approach to fighting disinformation has important *advantages* and *strengths*:

- It demonstrates the *willingness, commitment* and *determination* of a government to fight disinformation which also increases *public awareness.*
- A further advantage consists in the guarantee of (at least some) *state resources* dedicated to the fight against disinformation.
- Anti-disinformation state agencies maintain a substantial track record in *monitoring*, *analyzing* and, at times, *debunking* disinformation. The collection of expert knowledge in these institutions very often results in the creation of one or several *databases*, e.g. containing lists of known forgeries, actors and distributors of disinformation, narratives and topics, that can be consulted by other state agencies, policy makers and other clients.
- Counter-disinformation agencies have proven to be able to conduct efficient *horizontal communication* about disinformation, i.e. informing and sensitizing their governments to disinformation and providing a platform for the exchange of information, knowledge and experience.
- If adequately designed, managed and equipped, counter-disinformation agencies can function as *key actors in coordinating, combining and leading* any state's or organization's *fight against disinformation*.

On the other hand, the institutional approach to fighting disinformation also suffers from some *weaknesses* and *shortcomings* that need to be addressed:

- Although the presence of an interagency body can have a positive impact on coordinating the counter-disinformation activities of different government units, the prospective risk of *over-bureaucratization, slow administrative processes* and even *blockages* should be averted through the maintenance of streamlining and efficiency.

- The fight against disinformation and foreign influence has, to some extent at least, always had a strong component of security policy and intelligence work: uncovering secret actors, linking disinformation to state actors and interests and, where possible and necessary, engaging in law enforcement.

- However, the inherent *secrecy* of intelligence and security policy poses a problem: security services will most likely withhold at least some information in order not to threaten their own operations. This will be even more likely if a counter-disinformation agency is designed not only to distribute knowledge horizontally among government and state actors, but also engages in active public outreach, information campaigns and press work. Therefore, a process of closer collaboration and institutional linkages need to be forged between counter-disinformation units and the intelligence services, which can further lead to a change in operational culture.

- The success of any anti-disinformation agency in times of digital democracy will depend on the level of *trust or mistrust* of the government on the part of the population. Hence, no government should take public trust in its counter-disinformation efforts as a given and educating and informing the public represents one of the most important tasks of tackling propagandist activities. Todd Leventhal, a former member of the Active Measures Working Group and disinformation specialist, accordingly called for the *establishment of an additional nongovernmental institute of expert spokespersons who amend the efforts* of state institutions in countering disinformation, inform the public, debunk disinformation publicly and act as a point of contact for the media and public.[52]

Overall, the institutional approach represents a key player in the battle against disinformation, aiding and complementing civil societal initiatives aimed at promoting transparency in the informational field. Any government which seeks to establish a counter-disinformation agency however also needs to be aware of potential pitfalls and address them via an appropriate design and setup, resource endowment and robust public engagement.

Table 1. Summary of the key features of counter-disinformation government agencies

Counter-disinformation agency	Organizational design	Staff	Horizontal communication within government	Vertical communication and public outreach	Focus	Approach
AMWG	Interagency working group	> 15	x	x	Countering foreign disinformation	Security; Public diplomacy
GEC	Interagency body within State Department	Min. 119	x	x	Countering foreign disinformation	Security; Public diplomacy; Data analysis
EU-East StratCom Task Force	Department within EEAS	16	x	x	Countering foreign disinformation	Public diplomacy
AG Hybrid Germany	Interagency working group	unknown	x	-	Domestic security	Security policy
AA: Public Diplomacy & Strategic Communica-tion Germany	Department within Foreign Ministry	14	x	x	Countering foreign disinformation	Public diplomacy
MPF Sweden	Agency	40-60	x	x	Domestic resilience	Security; Public diplomacy
CCD Ukraine	Agency	52	x	x	Security	Security; Defense policy
VIGINUM France	Agency	42-60	x	-	Domestic security	Security policy; Data analysis
DCT Taiwan	Interagency unit	unknown	x	limited	Domestic resilience	Information policy

Endnotes

[1] Filipova, R., Nehring, C., 2023, *Effective Strategic Communications for Resilient State and Society A Conceptual and Institutional Blueprint*, Institute for Global Analytics, Briefing paper (2) September 2023 (https://globalanalytics-bg.org/2023/10/19/new-briefing-paper-effective-strategic-communications-for-resilient-state-and-society/).

[2] Schoen, F., Lamb, C., 2012, Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference, in *Strategic Perspectives* 11, (https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf); the author is also much obliged to former AWGP staff member Todd Leventhal who patiently answered numerous questions about the design, structure and modus operandi of the AMWG.

[3] Leventhal, T., 2020, What Can We Learn from the Active Measures Working Group?, in *GEC Counter-Disinformation Dispatches* #8, 2020 (https://e.america.gov/t/i-e-mjdiua-l-tr/);
Schoen, F., Lamb, C., 2012, Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference, in *Strategic Perspectives* 11, (https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf).

[4] Global Engagement Center, US Department of State, *About us* (https://www.state.gov/about-us-global-engagement-center-2/).

[5] Ibid.

[6] For example: Flade, F., 2022, Neue Lügen und alte Strategien, in *Verschlusssache. Über Spionage, Terrorismus und Sicherheitspolitik*, 30.8.2022 (https://ojihad.wordpress.com/2022/08/30/neue-lugen-und-alte-strategien/).

[7] Ibid; also: Müller, A., et al., 2023, Dreiste Desinformationskampagnen. Sie verbreiten Putins Lügen in Deutschland und was macht die Regierung?, in *Spiegel* (https://www.spiegel.de/politik/deutschland/dreiste-desinformationskampagnen-sie-verbreiten-putins-luegen-in-deutschland-und-was-macht-die-regierung-a-8fd1b720-bff1-4fa6-afe8-c946cfef6764), 16.2.2023.

[8] https://www.auswaertiges-amt.de/de/aussenpolitik/themen/-/2089138; also: Deutscher Bundestag, 2022, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Sevim Dağdelen und der Fraktion DIE LINKE. – Bundestagsdrucksache Nr.: 20/5092 vom 27.12.2022* (https://dserver.bundestag.de/btd/20/052/2005250.pdf), p. 5.

[9] "Weidemann, A., Das ist kein Spiel mehr, in *FAZ*, 4.1.2023, p. 11.

[10] VIGINUM, 2022, *Annual Report*, http://www.sgdsn.gouv.fr/rapport_thematique/viginum-annee1/.

[11] At the end of June 2022, the agency launched its first major recruitment process (VIGINUM, 2022, https://www.sgdsn.gouv.fr/publications/proteger-le-debat-public-numerique-viginum-recrute-ses-futurs-experts), thus suggesting that it took on its work with considerable less workforce during the first year of existence (which might also explain the scarcity of publicly available information and limited amount of activities). According to a recruitment website, in 2022 VIGINUM had only 42 employees (https://www.welcometothejungle.com/fr/companies/viginum).

[12] Alonso, P., Guiton, A., 2021, Les dessous de "Viginum", la future agence contre les manipulations de l'information, in *liberation*, 30.6.2021 (https://www.liberation.fr/societe/police-justice/les-dessous-de-viginum-la-future-agence-contre-les-manipulations-de-linformation-20210630_NF-TB6CNJ6ZGDDFBMZRZK/).

[13] Ibid.

[14] VIGINUM, 2022, *Annual Report* (https://www.sgdsn.gouv.fr/files/files/Publications/RA-Viginum-Annee1-32p-V20_EN_LQP-1.pdf).

[15] VIGINUM, 2023, *RRN: A Complex and Persistent Information Manipulation Campaign, 19*.6.2023 (https://ihedn.fr/en/2023/06/30/rnn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et-persistante/); also: Khatsenkova, S., 2023, 'Doppelganger': How France exposed a massive Russian disinformation campaign, in *Euronews*, 15.6.2023 (https://www.euronews.com/2023/06/15/doppelganger-how-france-exposed-a-massive-russian-disinformation-campaign).

[16] Schneider, A., 2022, Schwedische Behörde gegen Desinformation: Wir rechnen mit einem großen Knall, in *Spiegel*, 6.9.2022 (https://www.spiegel.de/ausland/schweden-wie-eine-behoerde-das-land-gegen-desinformationen-verteidigt-a-92422cee-4af9-4ab9-8ba2-5ed6d9f18e00).

[17] MPF, *Mission Statement*, https://www.mpf.se/en/mission/.

[18] MPF, *About us*, https://www.mpf.se/en/about-us/.

[19] Vilmer, J., 2021, *Effective state practices against disinformation: Four country case studies*, ed. Hybrid CoE, Helsinki (https://www.hybridcoe.fi/publications/hybrid-coe-research-report-2-effective-state-practices-against-disinformation-four-country-case-studies/) p. 10-14; also: Fjällhed, A. et al., 2021, A Swedish Perspective on Foreign Election Interference, in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, eds.: Ohlin, J., Hollis, D., Oxford, p. 139-161 (https://doi.org/10.1093/oso/9780197556979.003.0007); also: Pamment, J. (2022), Brand Sweden, in *Nation Branding. Concepts, Issues, Practice*, ed. Keith Dinnie, London, (https://doi.org/10.4324/9781003100249).

[20] Government of Sweden, 2023, *Pressträff om Sveriges säkerhet 31.1.2023* (https://www.regeringen.se/pressmeddelanden/2023/01/presstraff-om-sveriges-sakerhet/).

[21] On CCD's mission statement: Center for Countering Disinformation, *About* (https://cpd.gov.ua/en/docs/about-center-for-countering-disinformartion/).

[22] Center for Countering Disinformation, 2023, *Events* (https://cpd.gov.ua/en/events-en/the-center-for-countering-disinformation-conducted-a-series-of-trainings-for-representatives-of-the-regional-military-administration-and-the-regional-state-administration/).

[23] Center for Countering Disinformation, 2023, *Announcements* (https://cpd.gov.ua/en/announcements/the-center-in-cooperation-with-the-high-school-of-public-governance-held-an-educational-course-for-civil-servants-of-category-a/).

[24] Center for Countering Disinformation, 2023, *Announcements* (https://cpd.gov.ua/en/announcements/the-center-for-countering-disinformation-conducted-a-series-of-trainings-for-the-representatives-of-the-central-executive-bodies/).

[25] Center for Countering Disinformation, 2023, *Events* (https://cpd.gov.ua/en/events-en/a-workshop-for-employees-of-the-ssufscp-in-kyiv-was-held-on-april-7/).

[26] Center for Countering Disinformation, 2023, *Announcements* (https://cpd.gov.ua/en/announcements/on-march-1-intensive-training-course-was-held-for-energoatom/).

[27] Center for Countering Disinformation, 2023, *Articles* (https://cpd.gov.ua/en/category/articles-en/).

[28] Quincy Institute for Responsible Statecraft, 2022, *Disinformation Board List Misserves Ukraine's Democratic Aspirations* (https://quincyinst.org/press/disinformation-board-list-misserves-ukraines-democratic-aspirations/), 26.7.2022.

[29] For example: Digital Society Project, 2022, *Annual Survey for 2022* (http://digitalsocietyproject.org/data/).

[30] Rauchfleisch, A., et al. 2022, Taiwan's Public Discourse About Disinformation: The Role of Journalism, Academia, and Politics, in *Journalism Practice*, 18.8. 2022 (https://doi.org/10.1080/17512786.2022.2110928).

[31] See in extenso: Kao, S., 2021, Taiwan's Response to Disinformation. A Model for Coordination to Counter a Complicated Threat, in *NBR Special Report* no. 93 (https://www.nbr.org/publication/taiwans-response-to-disinformation-a-model-for-coordination-to-counter-a-complicated-threat/), p. 10.

[32] Ibid., p. 11, according to whom "the team has defined disinformation as information that satisfies three criteria: 1. Malice. When viewed subjectively, the disseminator of the information has malicious intent, driven by political or economic motives. 2. Falsehood. When viewed objectively, the content is demonstrably false. 3. Harm. The information leads to harmful consequences for personal, societal, or national interests."

[33] Executive Yuan, 2019, *Anti-Disinformation Policy Overview 2019* (https://www.tph.moj.gov.tw/media/205076/2019%E9%98%B2%E5%88%B6%E5%81%87%E8%A8%8A%E6%81%AF%E6%94%BF%E7%AD%96%E7%B0%A1%E4%BB%8B.pdf?mediaDL=true).

[34] According to Kao, S., 2021, *Taiwan's Response to Disinformation*, p. 14, DCT has developed four principles for debunking which they describe in detail: "a) *Humor over rumor*. All debunking messages shall be "packaged in such a way that the audiences cannot resist to share"—or in another word: "memefied".; b) *2-2-2 principle*. Each "memefied "debunking message shall contain no more than 20 characters in its title, no more than 200 characters in its content, and no more than 2 images appended; c) *Delayering*. Each debunking message, while "memefied" by the group of community editors set up by each agency, would be directly reviewed (or often instructed in advance) by the spokesperson of the agency (...); d) *Coordination in advance*. All spokespersons of agencies within the central government are highly connected as a "system." This system continuously monitors the circulating opinions of the public and decides which agency is best suited for responding to disputed information."

[35] Ibid., p. 15-18.

[36] Ibid., p. 18-22; see also: Baron, J. 2022, Ukraine Disinformation Fight Sounds Warning Bells for Taiwan, in *The Diplomat*, 23.6.2022 (https://thediplomat.com/2022/06/ukraine-disinformation-fight-sounds-warning-bells-for-taiwan/).

[37] E.g. by Germany's Federal Agency for Civic Education, 2022, *Podcast: Netz aus Lügen – Der Ausweg (7/8) Die globale Macht von Desinformation* (https://www.bpb.de/mediathek/audio/505063/netz-aus-luegen-der-ausweg-7-8/).

[38] Sass, M., 2022, How Taiwan is countering Chinese disinformation, in *Deutsche Welle*, 25.8.2022 (https://www.dw.com/en/how-taiwan-is-countering-chinese-disinformation/a-62931086).

[39] Kao, S., 2021, *Taiwan's Response to Disinformation*, p. 23.

[40] https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en.

[41] This analysis will, however, focus on their countering disinformation and FIMI efforts.

[42] Dausend., P., et al., 2017, Elf Aufrechte gegen Lügen. Eine Gruppe europäischer Beamter kämpft gegen Fake-News, in *Zeit online*, 19.1.2017 (https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2F2017%2F04%2Ffake-news-beamte-europa-kampf).

[43] EUvsDisinfo, https://euvsdisinfo.eu/about/.

[44] European External Action Service, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11248.

[45] Ibid.

[46] European External Action Service, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11266.

[47] European External Action Service, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11253.

[48] EUvsDisinfo, https://euvsdisinfo.eu/disinformation-cases/.

[49] European External Action Service, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11251.

[50] Ibid.

[51] It is noteworthy that the Task Force was subject to at least two big scandals: in 2018, it incorrectly identified articles by several Dutch news outlets as "Russian disinformation", prompting a counter-response by the Dutch government aiming to close down the Task Force (c.f.: Funke, D., 2018, *Three publications are suing the EU over fake news allegations*, Poynter Institute, 28.2.2018 (https://www.poynter.org/fact-checking/2018/three-publications-are-suing-the-eu-over-fake-news-allegations/); and in 2020 the Task Force was accused of having watered down a report on Chinese disinformation and influence operations due to political pressure (see: Razputo, M., 2020, Top E.U. Diplomat Says Disinformation Report Was Not Watered Down for China, in *New York Times*, 30.4.2020 (https://www.nytimes.com/2020/04/30/world/europe/coronavirus-china-eu-disinformation.html).

[52] Leventhal, T., 2023, The need to up our game in countering disinformation, in *Comparative Strategy* 42:2 2023, pp. 173-186.

t: +359 887 760 787
e: info@globalanalytics-bg.org
w: www.globalanalytics-bg.org
f: InstituteforGlobalAnalytics
in: www.linkedin.com/company/79841057