978-9934-619-13-7

A CAPABILITY DEFINITION AND ASSESSMENT FRAMEWORK FOR COUNTERING DISINFORMATION, INFORMATION INFLUENCE, AND FOREIGN INTERFERENCE

Published by the
NATO Strategic Communications
Centre of Excellence

ISBN: 978-9934-619-13-7
Author: James Pamment
Project manager: Henrik Twetman and Sara Sorensen
Design: Kārlis Ulmanis

Riga, November 2022
NATO STRATCOM COE
11b Kalnciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

Executive summary

This report proposes a capability assessment framework for countering disinformation, information influence, and foreign interference. At present, much emphasis is placed on the capability to counter disinformation and other associated phenomena. However, few have attempted to systematically define what those countermeasures are, and how they could be placed within a single, coherent capability assessment framework.

This lack is not least because countries do not, and should not, approach these challenges in the same way. Geography, history, political systems, areas of expertise, and relative power explain to some extent why countries use different terminologies, organisational structures, and policies for dealing with foreign interference. Furthermore, friendly actors at times share capabilities–such as tech platforms, researchers, non-governmental organisations (NGOs), and private-sector intelligence companies. There is no perfect template for assessing capabilities, but rather only organisations and systems designed to cope with different threats based on their mandates, interests, and available resources.

Since there is no one-size-fits-all solution to this problem, this report provides a flexible approach to capability assessment based on simple principles that can be applied by different types of actors. In support of this, and drawing upon previous research in this subject area, four capability assessment tools are established as tools to solve different assessment problems:

- *Objectives* are a cluster of capability measures associated with the explicit or implied purpose of an activity. Assessment can be developed, for example, from policy announcements, norms and expectations, and archetypical examples.

- *Indicators* weigh the factors that contribute to objectives, deconstructing them into constituent parts. Assessment can be developed, for example, from qualitative and quantitative measures, subjective and objective data, as well as from process measures such as response time, throughput, or success rate.

- *Risk assessments* prioritise anticipated vulnerabilities and threats and can help to assess preparedness for those scenarios.

- *Process maturity* assesses organisational and process efficiency on a scale that begins with ad hoc and unstructured practices and ends with highly optimised routines.

The capability assessment framework proposed in this report takes this toolset and applies it in three stages. First, disinformation, information influence, and foreign interference are defined. In the order shown, these three terms represent an escalating scale of breadth and strategic intent. Briefly, their generally accepted definitions are as follows:

- *Disinformation* refers to a group of activities where the intent and factualness of message content is in focus.

- *Information influence* refers to manipulative communication techniques used in support of an actor's goals.

- *Foreign interference* refers to efforts to achieve a hostile foreign actor's goals using hybrid methods including disinformation and/or information influence.

Second, these definitions are used to establish a basis for categorising countermeasures. Countermeasures are grouped into overall approaches and broken down into specific capabilities. Each group of countermeasures consists of several individual capabilities; in total, around 50 unique capabilities are defined according to this schema.

- Disinformation's main countermeasures involve the capability to determine and correct the factualness of messages (*correcting content*) and capabilities relevant to improving *public resilience* to misinformation and questionable sources.

- The main countermeasures for information influence involve more advanced *analysis and identification* capabilities as well as proactive *strategic communication* capabilities designed to push back on covert campaigns.

- The main countermeasures for foreign interference involve *intelligence* and *security policy* capabilities that are honed to deal with communicative threats.

- In addition, a further group of capabilities are included to cover system-wide questions, such as capabilities distributed across a *country-wide* system, shared capabilities within *partnerships and alliances*, as well as *staff development* capabilities.

The third layer of the framework provides general indications regarding which assessment methods from the aforementioned toolset are most applicable to each group of capabilities. Examples are suggested in a way that demonstrates the overall applicability of tools to different assessment challenges, rather than attempting to define a single solution. In most cases, a combination of two or more assessment tools will be relevant to most organisations.

The importance of taking steps toward a viable capability assessment framework should not be understated. Currently, there is much talk of a need for Counter-foreign interference capabilities at the political level, with limited efforts to understand how to assess and develop those capabilities at the level of individual tasks, at the scale of country systems, within formal and informal alliances, or for prioritised threat scenarios. The framework proposed here offers a modest step forward, without overly prescribing how assessment should be used, given the sensitivity of national differences.

Different types of organisations, including government departments and agencies, local government, NGOs, research organisations, intergovernmental alliances, tech companies, private-sector intelligence companies, and other stakeholders, can take inspiration from this framework to design a tailored schema for comparative capability assessment.

Contents

Introduction

Despite increasing attention dedicated to how issues such as disinformation, information influence, and foreign interference can be mitigated and countered, suitable terminology for categorising relative capabilities for counteracting these phenomena is lacking. As governments, public-sector agencies and institutions, non-governmental organisations (NGOs), and the private sector ramp up their counter-influence activities, the need to develop our understanding of what capability means in this field is increasing.

In relation to countering disinformation, information influence, and foreign interference, many synonyms are used to describe capability, but they often lack clarity as well as consistency. In particular, there is at present a significant gap when it comes to comparative assessment of capabilities at different levels—for example, the capability to perform individual tasks, such as debunking or attribution, versus systemic capabilities distributed between actors within countries or intergovernmental alliances. Concepts such as civilian defence and public-private partnerships imply a common perception of capabilities that at present simply does not exist.

This report seeks to develop a framework suitable for assessing capability in countering disinformation, information influence, and foreign interference. In doing so, it is focused upon the following questions:

- What methods can be used to assess capability?
- What are the main capabilities that should be assessed?

The report breaks new ground in three areas. The first is to establish a toolset of capability assessment methods, by conducting a brief literature review of the concept of capability as it has been applied to disinformation. The second establishes a framework for the comparative assessment of counter-disinformation capabilities, categorising 50 of the most relevant capabilities into manageable groups. The third suggests how the capability assessment toolset can be employed for each group of capabilities. Together, these contributions are intended to stimulate ideas about how such an approach can be applied to different organisations, based on their needs.

Capability assessment framework

In fields such as risk management and business management, capability is a central concept, useful not only for evidence-based policy but also for facilitating cooperation and knowledge development. In the simplest terms, capability refers to the ability to do something, to perform a task. It sits between an intention and an outcome. According to some classic business school definitions, it refers to the 'collective skills, abilities, and expertise of an organization' and is a way of defining what the organisation is and does.[1] More colloquially, it refers to what an organisation can and cannot do; for example, one may have a monitoring capability comprising trained staff and appropriate software, but lack the capability to use the data in a timely manner.

This report builds upon recent efforts to adapt capability assessment models to countering disinformation, information influence, and foreign interference, which are presented in three reports commissioned by the NATO Stratcom COE.[2] The report by Oxford Research[3] considers communication and policy implementation ability of local government organisations, and develops a list of skills and indicators that could be relevant to defining and assessing their Counter-information influence capability. The report by Pamment and Zemdega[4] establishes a pilot framework for evaluating the resilience of NATO alliance members to disinformation. The Lindbom[5] report introduces the 'new risk perspective' within risk management to suggest ideas for how these principles might be applied to information influence activities.

These three reports contribute to the discussion by demonstrating just how unique and challenging disinformation, information influence, and foreign interference are to deconstruct according to traditional capability assessment approaches. They provide much food for thought, while offering useful examples of practical ways forward. Drawing upon insights from all three reports, the framework proposed here combines four assessment tools: objectives, indicators, scenarios, and process maturity.

Objectives

While it may be a reasonable ambition to create a capability framework that allows for the comparison of country systems and their relative capabilities, in reality this task is all but impossible. Countries do not, and should not, approach these challenges in the same way. Geography, size, history, political systems, national interest, areas of expertise, and relative power explain these differences to some extent. While it may seem obvious to liberal

democracies that certain capabilities should be housed in a civilian ministry or public agency, countries with a colonial past may have good reason for not developing those capabilities, or prefer to rely on trusted partners to bolster capabilities. Countries with close proximity to a hostile power may emphasise, or deliberately de-emphasise, certain capabilities in conjunction with developments in their bilateral relationship. Put simply, there is no perfect template for capabilities, but rather only systems designed to cope with different vulnerabilities and threats based on available resources.

Objectives matter. This reasoning about vulnerabilities and threats is often expressed in a national security strategy or equivalent. Such documents establish exactly what a country seeks to protect. Indeed, amidst so much talk about the risks of foreign interference and disinformation, it is at times easy to lose track of exactly what we seek to protect. Therefore, including objectives in an assessment toolset can provide an essential foundation. For example, the 2017 Swedish National Security Strategy[6] establishes a number of national-level objectives, such as the following examples:

- To maintain foundational values, such a democracy, rule of law, and human rights; and
- To, under all circumstances, defend Sweden's freedom, security, and right to self-determination.

All three aforementioned reports note the importance of objectives when assessing capabilities, but none provide a comprehensive answer to how capabilities can be compared across, for example, country systems whose goals and methods take different forms. Nor are there reliable solutions for weighing the total comparative capabilities of holistic systems in an objective way.

Westerberg et al. (2021) assume a system-wide perspective on capability assessment, with the assumption that actors with responsibilities within civil defence, such as municipalities, regions, and county administrative boards, may lack the understanding, will, and capacity to implement government policy about disinformation. Their approach suggests that the existence of country-level desired skill categories, such as willingness or trust, can be used as indicators for capabilities, which can then be measured. However, this is not really the same thing as clear country-level objectives. This approach assumes a management perspective that heavily focuses upon organisational constraints against capability development, such as a lack of understanding of local government's role in civil defence. It does not go far enough, in terms of the objectives of this present report, in teasing out the specifics of countering information influence.

Indicators

Both Westerberg et al. (2021) and Pamment and Zemdega (2021) rely on indicators as

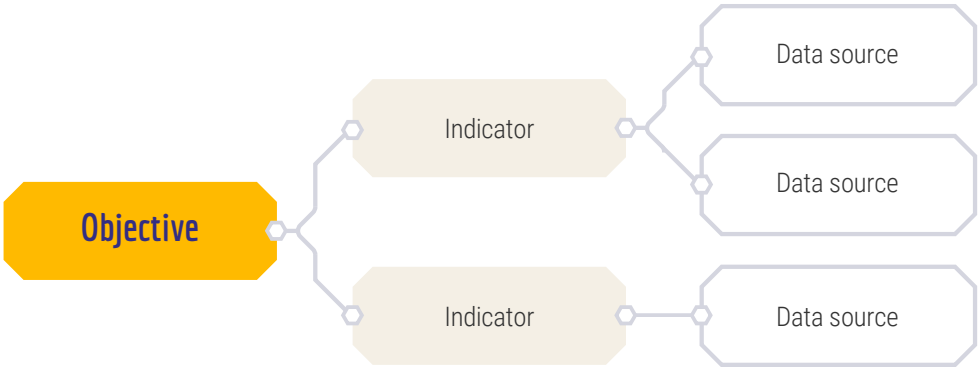

Figure: The links between objectives, indicators, and data sources

the main capability assessment method. Both studies use objectives, or proxies that can act as implied objectives, and attempt to operationalise them by dividing into measurable indicators. These indicators are then tied to data sources, such as self-reported qualitative data, independent indices, and public survey data, to provide data points for each indicator. In the latter report, each indicator is weighted to create a set of measures that are broadly comparable between alliance members.

One problem with applying this approach to the present project is a lack of equivalent data sources, which risks leaving indicators unmeasurable or at least with measures that are expensive to produce and mostly subjective. A second problem is accounting for national or organisational objectives related to capabilities that may not lead to comparable indicators. Lindbom (2022) acknowledges this limitation and argues that scenarios are needed to supplement an indicator-based approach. Scenarios provide additional means of assessment that are particularly relevant to risk-based assessment.

Scenarios

Lindbom (2022) advocates for a combination of resource management, process modelling, and risk management. A typical process-oriented capability model compares checklists of resources with likely scenarios or indicators based on risk projections. For example, a hospital might seek to calculate how many beds, doctors, and nurses it could muster given different types of stresses on its resources. Workloads on Saturday nights will be different compared to Wednesday afternoons. Response capabilities following a plane crash might be sufficient, whereas dealing with the long-term effects of a pandemic might stretch those resources too far. Rather than solely using indicators, establishing likely scenarios based on realistic threats is a relevant means of assessing capability.

From a management perspective, capability assessment facilitates decision making about appropriate resources based on different types of risk. Such assessment could involve a cost-benefit analysis (whether it is, for example, a sensible use of resources to have additional beds on standby) or use of rights-based criteria (such as if there is legislation stating that a certain number of doctors should be available per capita).[7] According to this approach, the role of risk management is to focus on the likelihood of adverse effects, their probable severity, and how they might impact both performance and objectives. The RESIST Toolkit published by the UK Government Communication Service advocates a similar approach, in which an organisation should establish threat scenarios[8] and prioritise countermeasures based on risk and likely harm.[9]

This approach provides a complementary method of assessment that overcomes the limitations of indicators. Rather than measuring the capabilities that are available, it places them within scenarios that demonstrate how prepared a system is to cope with different likely types of harm. Objectives still play a role, but this approach prioritises vulnerabilities and threats (and the capability to deal with them) ahead of policies, objectives, resources, and intentions.

Process maturity

Capability maturity models (CMMs) have been used since the 1980s to categorise the optimisation of software development processes.[10] Using a combination of diagnostic tools including, most importantly, a questionnaire, the model seeks to assess capabilities in different aspects of software development, from immature processes that are ad hoc, to evolved processes that are repeatable, defined, managed, and eventually optimised. The approach has inspired many areas of work outside of software development, including project management, organisational development, as well as public-sector capability assessments. While there is clearly no one-size-fits-all approach to assessing capability maturity in countering disinformation, information influence, and foreign interference, CMMs provide an additional layer of assessment tools that could be adapted to resolve specific assessment problems.

Figure: The levels of a capability maturity model

A pragmatic toolset

Based on the above analysis, it should be clear that no single approach copes well with the intangible aspects of strategic communication, not to mention the complexities of truth, influence, and intent in the context of espionage. Rather, it makes more sense to develop a vocabulary of approaches, each of which can be applied to different types of capabilities individually, and sometimes in combination. This affords some flexibility in how the framework can assess capability across the range of countermeasures relevant to disinformation, information influence, and foreign interference.

Objectives can be used as a cluster of capability measures associated with the explicit or implied purpose of an activity. Some tasks are best assessed by weighing them against what they are supposed to do. (For example, do public awareness campaigns make people more aware?) Assessment can be derived from sources such as policy announcements, vision statements, norms and expectations, or even archetypical examples. This approach typically takes the form of simple measures tied to a broad goal and is therefore unlikely to offer much nuance or detail, but it is useful for capturing the big picture.

Indicators can be deployed to weigh the factors that contribute to objectives, broken down into constituent parts. Capability assessment can be developed, for example,

from qualitative and quantitative measures, subjective and objective data, as well as from process measures such as response time, throughput, or success rate. This is useful for deconstructing tasks and establishing some baseline data, even if those measures are subjective or incomplete. An advantage of indicators is that more granular data can be compared across and between systems, for example in comparing different countries.

Risk assessments can support efforts to prioritise likely vulnerabilities and threats, and to assess preparedness for those scenarios. Rather than assessing single tasks or activities, it attempts to assume a holistic view over resource management within an interconnected system, to better understand how capabilities function together under stress. This adds a further dimension to the previous assessment tools, since objectives and indicators do not always acknowledge priority threat situations.

Process maturity allows for the assessment of organisational and process efficiency on a scale that begins with ad hoc and unstructured practices and ends with highly optimised processes. This complements other assessment tools by further pinpointing areas of relative strength or weakness, and offering suggestions for how they might be made more efficient.

Together, these four assessment tools constitute the overarching approach of the capability assessment framework proposed in this report.

Counter-disinformation capabilities

NATO's understanding of disinformation is aligned with the broader research community. It defines disinformation as the 'deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead'.[11] However, as recent studies have noted,[12] disinformation is often used as a synonym for two closely related terms: misinformation and malinformation. Misinformation refers to verifiably false information that is shared without an intent to mislead, whereas malinformation refers to true or partially true information that is twisted or taken out of context to support false interpretations.[13]

This group of terms can be characterised by an emphasis on information content. Analysis of this type of content weighs two factors: the factualness (or truth) of a message, and the likely intent behind the creation of the message. All three terms fit together under the disinformation umbrella, as a way of analysing factualness and intent based on message content.

Associated countermeasures are about correcting false information. Content moderation approaches, including fact-checking, debunking, and counter-messaging, are used to prove whether suspected content is true or false and to provide corrections where appropriate. General education of the public (in, for example, source criticism, media literacy, and prebunking) is used to strengthen societal resilience. Counter-disinformation capabilities may therefore be grouped in two broad buckets: content correction and public resilience.

Disinformation & associated concepts

Term	Misinformation	Disinformation	Malinformation
Definition	False information spread unintentionally	False information created intentionally	Factual information distorted intentionally
Operational components	Truth/factualness of content Intent of content creator		
Counter-measure capabilities	Content correction capabilities Public resilience-building capabilities		

Content correction

This refers to work specifically pertaining to false and/or misleading content, where the main required capabilities are to determine factualness and, in some cases, intent. Here, the main countering capabilities are therefore focused upon methods of content correction, which are surprisingly varied and established across a variety of stakeholders. These countering capabilities include the following:

- *Content moderation*: removal of problematic content based on rules/guidelines. Example: webpages with comment or user submission functions employ content moderation to ensure that offensive or illegal content is quickly removed.

- *Content flagging*: identifying and flagging problematic content to platform owner. Example: an NGO such as HateAid[14] is able to flag lists of identified hate speech examples to governments and platform owners.

- *Content labelling*: identifying and labelling problematic accounts and/or content. Example: Twitter adds a label to state media accounts[15] to inform users about the account ownership.

- *Content demotion*: developing mechanisms to cease algorithmic promotion of problematic content. Example: shortly after the Russian invasion of Ukraine, Meta created a policy to demote[16] Russian state media content on Facebook pages.

- *Fact-checking*: independent, nonpartisan review of content for errors. Example: Full Fact[17] checks a variety of official and news media statements about issues in the public interest.

- *Debunking*: targeted review of content and exposure of falsehoods. Example: Snopes[18] debunks common urban legends.

- *Counter-messaging*: targeted and direct exposure of falsehoods. Example: EUvsDisinfo[19] exposes and debunks disinformation as part of a campaign to raise awareness and push back against Russian disinformation in the EU.

- *Elves*: organised anti-troll network to actively correct false content. Example: in Lithuania[20], 5,000 volunteers work in a loose coalition to combat and expose false claims made by Russian disinformation.

Capability assessments of content correction can draw upon all four tools. The objectives of content correction activities are important to assessing whether those ca-

pabilities are fit for purpose. For example, a debunking team might limit its activities to a certain subject area, which means that capability is best assessed in relation to limited goals. Objectives may also be outcome-based (anticipating an impact such as reduced spread of disinformation in a topic area) or activity-based (focused upon producing a certain number of corrections in a certain time).

Assessment indicators for content correction focus on throughput, response volume, and resourcing levels. This is on the grounds that content correction is contingent upon the ability to process an appropriate amount of content, or at least to prioritise the most harmful types of content, in relation to an unpredictable amount of false content. Indicators are relatively straightforward to derive from the overall objectives, in order to establish measurable components.

Risk assessment would likely be centred on specific scenarios which require a mustering of resources, such as elections (predictable) or terrorist attacks (unpredictable). Scenarios such as pandemics or new conspiracies can be weighed against likelihood and risk and prioritised accordingly. Data from indicators can support assessment of likely performance in the face of these scenarios, with the additional possibility of tabletop exercises or other simulations aimed at testing capability. Finally, it is also possible to evaluate previous activities in relation to, for example, COVID-19 or recent elections to assess capabilities and propose improvements.

Some processes, such as data collection and handling around fact-checking and debunking, can be assessed in terms of process maturity. For example, the process by which cases are flagged and responded to can be optimised to improve throughput.

Public resilience

This refers to work specifically related to informing the public about the risks posed by false or misleading content and strengthening their ability to recognise it. The main countering capabilities are therefore focused upon educational and informational interventions designed to improve the resilience of groups and individuals, which include the following:

- *Public awareness-raising campaign*: domestic-focused information campaign about threats and threat methods. Example: the Swedish Psychological Defence Agency[21] created a public awareness campaign in the run-in to the 2022 general election called 'don't get fooled '.[22]

- *Media literacy*: education or training in how to critically interpret media. Example: the European Digital Media Observatory includes a substantial effort[23] to map, and build capacity, for media literacy initiatives in Europe.

- *Source criticism*: education or training in critically evaluating information sources. Example: NewsGuard[24] is a web browser plugin that gives trustworthiness ratings for news sources, based on criteria such as credibility and transparency.

- *Prebunking*: targeted efforts to prepare audiences to reject harmful falsehoods. Example: during the COVID-19 pandemic, researchers prepared a guide[25] for dealing with vaccine hesitancy, designed to pre-empt likely fears and misgivings with interventions based on factual information.

Capability assessments are therefore likely to be indicator-based. They would, for example, emphasise the reach of such initiatives and combine it with survey data about, for example, public confidence in their ability to identify disinformation. An EU Barometer survey[26] did the latter in 2018, offering possible insight into how the EU public views the threat from disinformation.

Risk assessments can centre on credibility and reputational damage that could affect public trust in organisations, such as government departments, and institutions, such as scientific research, in certain scenarios. Prioritising these threats could help to establish whether prebunking capabilities, as well as overall resilience levels, are sufficient. These assessment methods can form a feedback loop that ensures efforts are adjusted for relevance and efficiency. Finally, process maturity could help to establish the effectiveness of teaching methods and materials, and hone, for example, train-the-trainer initiatives.

Counter-information influence capabilities

In Sweden, information influence is a term mainly used to define efforts to influence democratic processes using illegitimate, but not necessarily illegal, methods to the benefit of foreign powers. The main differences between information influence and disinformation reside in the operational components. Whereas disinformation emphasises factualness and intent in the content of messages, information influence emphasises the communication techniques that make up a coordinated effort to influence a society, their manipulative components, and the objectives of those conducting them.[27]

Information influence therefore encompasses disinformation and its associated terms as possible tactics, but predominantly refers to a broader set of coordinated actions, to which factualness is subordinate, and intent is already established as hostile. However, as an example, it is worth noting that Swedish law only offers a mandate for government agencies to investigate information influence when there is suspicion that the activities are conducted by or on behalf of a hostile foreign actor. For the purposes of this section, it makes more sense to focus on objectives that are to the benefit of a hostile actor in a general sense, and to leave the specifics of the foreign power aspect for the final category of definitions (foreign interference) discussed later in this report.

There is further conceptual justification for making this small distinction. Information influence is similar to the French use of the terminology "information manipulation". In their comprehensive analysis of this policy area, Vilmer et al. establish that information manipulation is by definition intentional and clandestine. This relates closely to the idea that the communication techniques used are illegitimate; they do not fit within the accepted norms of public discourse insofar as they are deceptive, covert, and seek to cause harm. Furthermore, this definition encompasses the criteria of being coordinated and making use of false or misleading information as a possible tactic. The intent to cause harm is often political but is not limited to only political harm.[28] France would later adapt this term into law,[29] and the EU has more recently integrated the term into its updated disinformation policy.[30] Whether the hostile actor is state-based or not is not central to the definition.

The present report assumes an agnostic view on the interests that motivate use of illegitimate communication methods. This is motivated by three factors. First, the definitions explained above are contingent

on national legislation, which means that their scope is in part defined by domestic political considerations. This is not helpful in dealing with terminology from an alliance-wide perspective; therefore, a report such as this needs to be able to step outside of national preoccupations. Second, it is increasingly clear that private and non-governmental actors are active in producing information influence, and that a definition of covert, coordinated campaigns by organisations without state backing is needed. A similar distinction has, for example, recently been made in relation to EU disinformation policy.[31] Third, assuming an agnostic view of the actors conducting this type of activity brings the definition closer to traditional views of propaganda as supporting any interest. Such definitions remain viable in the digital age. For example, Facebook's definition of influence operations as 'coordinated efforts to manipulate or corrupt public debate for a strategic goal' is actor-agnostic.[32]

Countermeasures to information influence are in part about the internal analytical capacity to understand the covert threat, and in part about communicative responses. For example, it would be desirable to possess the capability to produce situational awareness and risk assessments to prepare a country or organisation for certain types of threats. The ability to rigorously investigate those cases is also essential. Regarding communicative response, common countermeasures include making the public familiar with certain types of threats through an awareness-raising campaign, developing counternarratives to contest the stories that adversaries are telling, as well as developing ways of dissuading or levying reputational costs on the hostile actors for their behaviour. This includes attribution, which is a capability in many respects contingent on others, such as investigative capabilities.

Information influence & associated concepts

Term	Information influence	Information manipulation	Influence operation
Definition	Illegitimate communication intended to influence society to the benefit of hostile foreign powers	Coordinated efforts involving the diffusion of false or distorted information with the intent to cause political harm	Coordinated efforts to manipulate or corrupt public debate for a strategic goal
Operational components	Intent to cause harm to the benefit of hostile actor Use of illegitimate communication techniques Negative interference in public debate Covert coordination		
Counter-measure capabilities	Analysis and identification capabilities Strategic communication capabilities		

Analysis and identification

This capability refers to work specifically related to analysing covert, coordinated efforts to negatively impact public discourse. The following main countering capabilities are therefore focused upon identification and risk assessment:

- *Monitoring*: processes for systematic monitoring of relevant policy areas. Example: the UK Rapid Response Unit[33] utilises a variety of digital analysis tools to enable the ongoing detection of disinformation related to, for example, COVID-19.

- *Situational awareness*: continual shared updates about trends in the information environment. Example: the Lithuanian Armed Forces[34] conducts digital monitoring of Russian propaganda in order to inform a cross-government response.

- *Threat assessment*: continual shared updates about threat tactics. Example: the US Office of the Director of National Intelligence, like many other intelligence agencies internationally, publishes annual threat assessments,[35] which include information influence and foreign interference.

- *Risk assessment*: develop preparedness and contingency planning. Example: the RESIST Counter-Disinformation Toolkit[36] outlines a process for conducting risk assessment for disinformation targeting government departments and their areas of responsibility.

- *Investigation*: investigate cases using rigorous and valid research methods. Example: the Atlantic Council Digital Forensic Research Lab[37] has a project called Digital Sherlocks[38] that seeks to train analysts and develop best practices for digital investigations.

- *Tabletop exercises (TTX)*: run scenario-based TTX to test capabilities. Example: the Helsinki-based Hybrid COE regularly holds joint EU-NATO tabletop exercises for training purposes as well as workshops[39] on how to design effective exercises.

- *Partnerships*: regular meetings with partners and allies with relevant information or capabilities. Example: the EU Rapid Alert System[40] is a meeting place for EU members to share knowledge about disinformation trends, new research, and effective countermeasures.

Analysis and identification capability assessments can draw upon all four tools. The objectives of the relevant capabilities can be outlined in terms of expectations, for example the speed and accuracy of monitoring and quality of analysis. These are by and large subjective, qualitative measures, since the usefulness of briefings

> Capability refers to the ability to do something, to perform a task. It sits between an intention and an outcome.

and shared assessments is very much in the eye of the beholder. Indicators can support assessment by offering details about frequency, volume, accounts tracked, staff resources, and software, for example. These resource overviews can be compared across similar teams in different countries or compared to ideal types.

Risk assessment could, for example, emphasise sudden changes in tactics and actors, which could evade established processes and systems. For instance, would the monitoring systems pick up these changes, or how would the threat assessment system respond to this or that scenario? The assessment can be combined with capability maturity models that assess the bureaucratic maturity of monitoring and threat sharing systems. In some cases, however, governments prefer to withhold details of their analysis capabilities because of security concerns, so it is likely such capability assessments would be for internal use only and confidential.

Strategic communication

This capability refers to work specifically related to the ability to communicate about, or in response to, a coordinated threat. The main countering capabilities are therefore focused upon persuasive communication designed to push back on the disinformation efforts, which include the following:

- *Content correction:* See content correction section above / refers to page X
- *Public resilience*: See public resilience section above / refers to page X
- *Proactive strategic communication*: run public diplomacy and other strategic advocacy campaigns abroad. Example: in response to COVID-19 misinformation, the World Health Organization, BBC, and the UK government partnered to create an advocacy campaign[41] which included a Mythbusters[42] database and advice on how to report vaccine misinformation to social media platforms.
- *Counter-narrative*: communications that contest established adversarial narratives. Example: in addition to debunking pro-Kremlin disinformation, EUvsDisinfo also publishes deeper analyses of themes that regularly occur

in Russian propaganda narratives, such as historical revisionism about the Second World War[43] and Ukraine.[44]

- *Counter-brand*: communications that expose or levy reputational costs upon a hostile actor. Example: the Global Coalition against Daesh[45] ran communication campaigns including efforts to counter-brand by exposing the differences between the propaganda and the realities of life under Daesh.

- *Published analysis*: report or working paper outlining a hostile campaign's methods. NATO Stratcom COE[46] regularly publishes reports that provide expert analysis of information influence campaigns and other related topics.

- *Attribution*: publicly assign blame to actor. Example: the Disinfodex[47] database houses over 300 disclosures made by tech companies about actors–state or nonstate–who have conducted influence operations on their platforms.

Capability assessments are challenging because strategic communication is notoriously difficult to evaluate accurately. Assessment based on objectives may have some value, such as in assessing impact and outcomes. Are we able to use the counter-brand approach effectively? This question is typically answered by capturing examples of communication activities and comparing them with any follow-ups or evaluations commissioned by the communication teams. If the communication team has used the OASIS model[48] (or an equivalent) for communication planning, relevant metrics may be available.

Indicators can cover three areas: organisational capabilities (number of staff, advertising budget, skills and training, etc.); communication capabilities (audience reach, campaign evaluations, awards, historical case studies, etc.); and response capabilities (the ability to change perceptions or behaviour in response to a specific and immediate threat). It is important not to confuse these levels since follow-ups of communication activities do not equate to a capability assessment. In some cases, however, governments prefer to classify details of their proactive communication campaigns, which adds a layer of complexity to assessment.

Perhaps a more robust assessment tool is risk assessment, which would question how well communication capabilities can respond to risks such as the COVID-19 infodemic. Here, there should be recent and compelling examples of lessons learned that can help to better understand capabilities under stress. A second relevant area of risk assessment is in questions of when, how, and whether to communicate, whom to partner with, and which actors should be named. This can be tested in tabletop exercises. Finally, process maturity, such as in the existence of formalised training and guidelines, could further help to establish more general capability levels.

Counter-foreign interference capabilities

The third area of capabilities covered in this report pertains to countering foreign interference. This area builds upon the themes covered in disinformation and information influence by adding two additional factors. First is the assumption that the activities within this category, no matter who conducts them, are ultimately carried out on behalf of a hostile state actor. Second, the communication activities broadly considered to be under foreign interference go beyond information per se and fit into the broader category of hybrid threats.[49] This imparts an additional layer of complexity upon disinformation or information influence that positions the communication activities within a set of covert tools for generating geopolitical influence.

According to a recent report commissioned by the European External Action Service, foreign interference should be defined as 'coercive, deceptive, and/or nontransparent efforts—during elections, for example—to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents.'[50] This allows for a distinction between disinformation and information influence conducted in support of the political and commercial goals of individuals, the private sector, and NGOs, versus disinformation and information influence conducted in the interests of a hostile foreign state. It is conceivable that some activities could simultaneously fit into both areas; still, a distinction is relevant, since the depth of diplomatic engagements with states enables different types of countermeasures to be used. Countermeasures can be developed to focus on the bilateral relationship from a holistic perspective. Furthermore, a hostile state involved in information influence is likely to also be using other hybrid influence methods, which are used in a combined manner to boost each other's effect.

Countermeasures involve areas related to intelligence as it pertains to the ability to track and assess the actors conducting information influence. For example, there is a heightened need to develop mechanisms for sharing relevant intelligence between the private sector, research, NGOs, as well as allied states. Open-source intelligence (OSINT) plays a prominent role, including the ability to rapidly declassify intelligence, and, likewise, counterintelligence as it pertains to domestic proxies supporting foreign information influence. On the security policy side is an intensified need to position countermeasures, including those mentioned in the previous areas, in the context of an actor-specific deterrence strategy. Tools such as attribution, sanctions, and even covert offensive operations constitute a range of capabilities to respond proactively to a hostile state.

Foreign interference

Term	Foreign interference
Definition	Disinformation, information influence, and other hybrid influence methods conducted by or on behalf of a hostile foreign state actor
Operational components	Intent to cause harm to the benefit of hostile state Use of illegitimate communication techniques Negative interference in public debate Covert coordination Deployment in coordination with other hybrid influence methods
Counter-measure capabilities	Intelligence: collecting, processing, and use capabilities Security Policy: actor-specific capabilities

Intelligence

This refers to collecting and processing of intelligence relevant to information influence in the context of hostile state actors. The main countering capabilities are therefore focused upon the ability to use intelligence effectively for these types of threats.

- *Analysis & identification:* See analysis and identification section above; however, in this case, this would refer to information influence analysis centres housed by intelligence agencies as well as their relevant mandates, such as a military intelligence focus.
- *Oversight*: a hub or fusion cell where data on these questions are collected and analysed.
- *Intelligence sharing:* ability to share classified intelligence with partners.

  Example: the NATO Intelligence Fusion Centre[51] allows Alliance members to share all-source intelligence materials to support NATO activities.
- *OSINT*: ability to work with open sources and/or rapid intelligence declassification. Example: following the Salisbury poisonings, Bellingcat[52] made use of open, leaked, and declassified intelligence sources to identify the alleged perpetrators.
- *Counterintelligence*: specialism in identifying domestic proxies who conduct information influence on behalf of hostile foreign states. The FBI[53] includes disinformation alongside other aspects of foreign interference as part of its counterintelligence work.

Capability assessments already exist specific to intelligence work, so the focus is

more likely to rest on the availability and timeliness of intelligence relevant to countering information influence, for example through surveys of intelligence customers throughout government. In many cases, governments withhold details of their intelligence-sharing capabilities for security reasons. Risk assessments would probably focus on high-priority national security threats and vulnerabilities. Others could consider the integrity of intelligence collection and protection of sources in the context of wider intelligence sharing and declassification. Overall, this capability is best assessed with existing methods used in other capability areas, with the addition of intelligence agency participation in other capability assessments to the degree that their activities perform a relevant role.

Security policy

This refers to work related to security issues as they are approached by, for example, security policy teams within governments whose main task is to assess state threats. The main countering capabilities are therefore focused upon the levers of statecraft that can be deployed in relation to information influence threats.

- *Deterrence*: coordinated efforts to influence a hostile state's calculus. Example: in 2020, the Hybrid COE launched a Deterrence Playbook[54] designed to support its members' efforts to systematically deter hybrid attacks.
- *Exposure*: like prebunking but informed by intelligence and security policy rationales to influence the calculus of a hostile state actor. Example: prior to the Russian invasion of Ukraine in February 2022, the US and UK released intelligence suggesting that Russia intended to use so-called false flag operations[55] as a pretext for war. Exposing these plans pre-emptively reduced Russia's opportunities for using such pretexts.
- *Attribution*: technical and political capabilities to assign blame to states and proxies. Example: the so-called Mueller Report[56] on Russian interference in the 2016 US Presidential Election proves systematic efforts by Russia and its proxies to influence the outcome of the election.
- *Network disruption*: use of cyber capabilities to disrupt an adversary's network. Example: during the 2018 midterm elections, the US allegedly disrupted the internet access[57] of the notorious St. Petersburg troll farm behind the 2016 election interference, the Internet Research Agency.
- *Legislation*: specific laws that empower government agencies to act proactively. For instance, Australia has the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 and Singapore has the Foreign

> Capability assessments are challenging because strategic communication is notoriously difficult to evaluate accurately.

Interference (Countermeasures) Act.

- *Sanctions*: levy costs upon hostile state and its agents. Example: in March 2022, the EU imposed sanctions[58] on Russian state media, including RT and Sputnik, in response to disinformation spread about Ukraine prior to and during the invasion.

- *Offensive operations*: run covert, coordinated influence operations abroad against a hostile state or its agents. Example: many armed forces possess the capability to run influence operations targeting adversaries in conflict zones. What used to be known as Psychological Operations (PsyOps) is increasingly referred to by NATO as Cognitive Warfare.[59]

Capability assessments are once again challenging in this particular area. Objectives and indicators can help to establish the appropriate size of teams, their resources, the existence of up-to-date country strategies, and the satisfaction of stakeholders within government, such as ministers. Given the nature of the tasks, risk assessments are valuable both for investigating various possible priorities and for assessing, from a holistic perspective, which types of scenarios are likely, and which capabilities should be frequently tested. Scenarios are likely to centre on the will, opportunity, and capability of hostile states to act, the vulnerabilities inherent to a specific society, and the impact countermeasures might have on already challenging bilateral relationships. The ability to appropriately produce and follow, and indeed know when to deviate from, a country-specific or policy-specific strategy is also a capability to be assessed. However, these are perhaps more questions of good judgement than capability per se. Evaluations of activity would also be valuable but are likely to be classified or lacking in detail relevant to determining capability. Process maturity could be a valuable means of assessing the extent to which activities are planned, proactive, and managed, as opposed to ad hoc activities and responses to ongoing crises.

System-wide capabilities

While the previous groups of capabilities are tied to definitions of specific problem areas and associated tasks, an additional category of capabilities is required to cover a broader subset of systemic questions. These systemic questions involve three key areas of capability: within the national system (or cross-government), as part of international and nongovernmental communities, and in terms of professional skills and professional development.

Country system

At the national level, capabilities involve the specific development of doctrine, terminology, and oversight within a national system and based upon culturally specific norms and laws. As previously mentioned, France and Sweden, to provide two examples, have their own terminology that is linked to long-standing philosophical and legal traditions, and which provides the basis for the contemporary iteration of what is now commonly called disinformation policy. Most countries have provisions for certain concepts in their laws and regulatory powers, which in turn sets the agenda for government departments and agencies leading that work. Development of those concepts, through research and development, revised legislation, and measurement and evaluation efforts, are key to ensuring that the national system remains robust in the face of emerging challenges. Some other connected areas, such as intelligence sharing and analysis capabilities, are covered elsewhere, but it is also essential to factor in civil defence as a whole-of-country capability connected to public resilience but more extensive in structure.

- *Research & development*: knowledge production focused on a country system through concept development, key publications, or technical contributions to the field. For example, independent research institutes with close ties to government are important for convening national debates through publications such as white papers and non-papers.

- *Legislation, regulation, & policy*: significant development of legal and practical basis for countermeasures.

- *Measurement & evaluation*: efforts to evaluate effectiveness or impact of countermeasures.

- *Coordination*: the ability to coordinate different actors to specific ends, for example in support of a national exercise or national capability assessment.

- *Civil defence*: doctrine, organisation, and established practices of civil preparedness and civilian defence.

- *Vulnerability analysis*: to what extent are there comprehensive efforts to map and monitor known areas of societal vulnerability.

Capability assessments will depend very much on how developed the country system is in these areas. Objectives and indicators are likely to emphasise specific contributions to the national understanding and handling of these issues, such as the development of legislation or new policies governing issues as broad as social media platforms, civil preparedness funding, and counterespionage. Coordination and civil defence are well suited to scenario-based risk assessments. Process maturity could be a useful means of assessing capabilities within, for example, local government, as a complement to use of indicators.

Partnerships and alliances

Intergovernmental and nongovernmental alliances are a crucial area of capability. International partnerships such as the G7 Rapid Response Mechanism act as hubs for collecting best practices, creating activity sharing programmes, and improving collective situational awareness. Likewise, partnerships with nongovernmental organisations such as social media companies, media houses, NGOs, think tanks, and universities can add significant capabilities to a network.

- *Governmental memberships & network participation*: participation in relevant bilateral, multilateral, and intergovernmental working groups and coalitions, including network leadership or hosting.

- *Nongovernmental partnerships*: research, private sector, and other relevant nongovernmental partnerships.

- *Joint initiatives*: participation in joint projects, including access to and use of additional external capabilities within these networked projects.

- *Common goods*: the capabilities your organisation adds to the network (for example, monitoring capabilities in a certain language) versus the capabilities accessed through the network (for example an enhanced investigation and attribution capability).

Capability assessments in this area are likely to emphasise the objectives of specific alliance groupings and one's own role in them. It would be relevant to develop indicators for the number of agreements and joint projects and to weigh the capabilities they add, or their relative importance to a given case or policy area. Risk assessments are a relevant means of testing joint capabilities.

Professional development

This area refers to staff capabilities and the support that staff receive to develop specialisations in areas of work relevant to these tasks. Professional development can be tailored for each industry so they can understand the threat that they face. A person working for a bank will face different threats from a person working in the media.

- *Guidelines*: shared best practice, guidance, toolkits, or other work to strengthen staff capabilities at a general level.

- *Specialism*: development of, for example, tailored training programmes, further education courses, or a career specialism track related to these issues.

- *Exchanges*: temporary secondments and exchanges for skill development, both inwards and outwards.

Capability assessments could emphasise indicators, such as the availability of personal development opportunities and the number of places available compared to, for example, the number who apply. Needs could be assessed against risk assessments which outline potential likely staff skill requirements given different scenarios.

> There is value in establishing the principles for a holistic framework, even if a great deal of further unpacking is deferred into future work.

Conclusion

This report charts a course for how to build a capability assessment framework for countering disinformation, information influence, and foreign interference. It is necessarily dense and covers a lot of ground in a small number of pages. There is much to unpack here: each section would be worthy of its own separate report. Additionally, implementation might not be easy. It may be necessary to add or remove specific terms or capabilities due to differences in mandates. It may be appropriate for some to add cyber, crisis response, critical infrastructure protection, or other categories of capabilities into the mix depending on how a given system is set up.

However, there is value in establishing the principles for a holistic framework, even if a great deal of further unpacking is deferred into future work. The idea is that this framework can be used to support many aspects of Counter-foreign interference policy and operations. By establishing a toolset for assessment, a breakdown of countermeasures, and indications of how capability assessment can be applied, the hope is that NATO allies and partner states can improve their efforts to counter foreign interference, both individually and as part of a collective. A single report such as this cannot provide all the answers, but it can begin to set out the right questions, using a structure that can be adapted to suit different types of needs.

Endnotes

1 Norm Smallwood and Dave Ulrich (2004) Capitalizing on Capabilities. *Harvard Business Review*. https://hbr.org/2004/06/capitalizing-on-capabilities

2 Note that only one of these reports is available to the public through the NATO Stratcom COE website.

3 Thomas Westerberg, Maja von Beckerath, Ylva Grauers Berggren (2021) Measuring the Ability of Local and Regional Actors to Counter Information Influence Activities. Riga: NATO Strategic Communications Centre of Excellence (unpublished).

4 Pamment, James & Zemdega, Riga (2021) Framework to Evaluate NATO Allies' Resilience to Disinformation. Riga: NATO Strategic Communications Centre of Excellence (unpublished).

5 Lindbom, Hanna (2022) Capability Assessment for Stratcom. Using the new risk perspective to inform the development of effective response capability assessments for countering information influence operations. Riga: NATO Strategic Communications Centre of Excellence.

6 Regerinskansliet Statsrådsberedningen (2017) Nationell säkerhetsstrategi. www.regeringen.se

7 Lindbom, *Capability Assessment for Stratcom,* p.16

8 Sometimes also referred to a "red teaming".

9 Pamment, James (2021) RESIST 2. London: UK Government Communication Service. Available at https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/

10 Paulk, Mark., Curtis, William., Chrissis, Mary Beth., & Weber, Charles. (1993). *Capability Maturity Model for Software (Version 1.1)* (CMU/SEI-93-TR-024). Retrieved 2022, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=11955

11 NATO's approach to countering disinformation: a focus on COVID-19, available at https://www.nato.int/cps/en/natohq/177273.htm

12 Pamment, James (2020) The EU's Role in Fighting Disinformation: Taking Back the Initiative (Part 1). Washington DC: Carnegie Endowment for International Peace. Available at https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

13 Pamment (2021) *RESIST 2*.

14 https://hateaid.org/

15 https://www.washingtonpost.com/politics/2020/11/05/technology-202-trump-twitter-feed-is-covered-warning-labels/

16 https://twitter.com/ngleicher/status/1498714352232239105

17 https://fullfact.org/facts/

18 http://www.snopes.com/

19 https://euvsdisinfo.eu/

20 https://www.debunkeu.org/about-elves

21 https://www.mpf.se/

22 https://www.bliintelurad.se/

23 https://edmo.eu/media-literacy/

24 https://www.newsguardtech.com/

25 https://www.movementdisorders.org/MDS-Files1/The_COVID-19_Vaccine_Communication_Handbook.pdf

26 https://data.europa.eu/data/datasets/s2183_464_eng?locale=en

27 Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018) Countering Information Influence Activities: The State of the Art. Swedish Civil Contingencies Agency (MSB). Stockholm: MSB. Available at https://www.msb.se/sv/publikationer/countering-information-influence-activities--the-state-of-the-art-research-report/

28 J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, pp. 20-22.

29 Guillaume, Marine (2019) Combating the manipulation of information – a French case (Hybrid CoE Strategic Analysis 16). Helsinki: Hybrid COE. Available at https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_16_manipulation-of-information_.pdf

30 Council of the EU (2022) Council conclusions on a Framework for a coordinated EU response to hybrid campaigns. Available at https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

31 Pamment, *The EU's Role in Fighting Disinformation*; European External Action Service (2021) Tackling Disinformation, Foreign Information Manipulation & Interference. Available at https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

32 Facebook (2021) Threat Report The State of Influence Operations 2017-2020. No place of publication. Available at https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

33 https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online

34 https://www.vice.com/en/article/59emgz/meet-the-colonel-in-charge-of-countering-russian-propaganda-in-lithuania
35 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
36 https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/
37 https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/
38 https://www.digitalsherlocks.org/
39 https://www.hybridcoe.fi/news/hybrid-coe-conducting-hyfutec-ttx-design-workshop-in-vienna/
40 https://www.eeas.europa.eu/node/59644_en
41 https://www.who.int/news-room/feature-stories/detail/countering-misinformation-about-covid-19
42 https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters
43 https://euvsdisinfo.eu/in-the-shadow-of-revised-history/
44 https://euvsdisinfo.eu/back-to-basics-ukraine-revisionism-and-russophobia/
45 https://www.gov.uk/government/topical-events/daesh/about
46 https://stratcomcoe.org/publications
47 https://disinfodex.org/
48 https://gcs.civilservice.gov.uk/guidance/marketing/delivering-government-campaigns/guide-to-campaign-planning-oasis/
49 Örden, Hedvig & Pamment, James (2021) What is so Foreign about Foreign Influence Operations? Washington DC: Carnegie Endowment for International Peace
50 Pamment, James (2020) The EU's Role in Fighting Disinformation: An EU disinformation framework (Part 2). Washington DC: Carnegie Endowment for International Peace, p. 5
51 https://web.ifc.bices.org/
52 https://www.bellingcat.com/tag/skripal/
53 https://www.fbi.gov/investigate/counterintelligence/foreign-influence
54 https://www.hybridcoe.fi/news/hybrid-coe-launches-a-playbook-on-hybrid-deterrence/
55 https://www.bbc.com/news/60470089
56 https://www.justice.gov/archives/sco/file/1373816/download
57 https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html
58 https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/
59 https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org