978-9934-564-38-3

STRATEGIC COMMUNICATIONS HYBRID THREATS TOOLKIT

Applying the principles of NATO Strategic Communications to understand and counter grey zone threats

PUBLISHED BY THE
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

ISBN: 978-9934-564-38-3

Editor: Ben Heap.

Researchers: Pia Hansen, Monika Gill.

Strategic Communications Hybrid Threats Toolkit
Applying the principles of NATO Strategic Communications to understand and counter grey zone threats.

Table of Contents

ABOUT THIS REPORT

This research is for people who want to develop their understanding of dangers to national security that come under the umbrella of 'hybrid threats'. Such threats involve a combination of different hostile measures, furthering an adversary's strategic goals while occuring in the 'grey zone' which exists between peace, crisis and war.

The report builds on our publication *Hybrid Threats - A Strategic Communications perspective,* which analysed 30 scenarios featuring hybrid activities by state actors. Data from the case studies is exploited further, deepening our understanding of hybrid threats and how they might be countered by applying the principles of NATO Strategic Communications. It aims to help the reader develop ways of looking at hybrid threats and then to appreciate how the Strategic Communications process might be applied at the national level. This involves understanding the information environment, then developing a plan which provides coherence to the various instruments a nation can use to leverage strategic influence.

Strategic Communications is a realm which suffers from a divergence of definitional interpretations. While NATO Strategic Communications has arguably come of age, there is understandably a lack of commonality across the NATO nations as to how the term is used. Popular usage has Strategic Communications simply as being highly effective at what an organisation *says*. This confines communication to a narrow arena. Our report builds on NATO's approach to Strategic Communications - a mindset or philosophy which is underpinned by process and supported by capabilities. When applied at the national level it provides a function of basic statecraft at the intersection of strategy and action.

The complex and adaptive nature of the contemporary security environment and its consequent unpredictability means that responses which work in one situation may not work in another. While not prescriptive or authoritative, our research provides suggestions on how to view the threat landscape, using empirical evidence in support. It provides methods and background information suitable for education and training for those in security-related areas of national government.

Acknowledgements. ***Project lead*** Ben Heap. ***Researchers*** Pia Hansen, Monika Gill. ***Thanks to*** Rolf Fredheim, Henrik Twetman, Sanda Svetoka, Johannes Wiedemann, Grzegorz Lyko.

> We live in a completely different security environment with a more blurred line between peace and war.

Jens Stoltenberg, NATO Secretary General[1]

1. INTRODUCTION

STRATEGIC CONTEXT

Changes in the international security environment continue to challenge our ability to understand and respond to the evolving landscape of threats. Traditional assumptions of what was once understood to be conditions of peace, crisis and war, with relatively clear boundaries in between, are increasingly no longer valid. The norms and laws governing the international system are being challenged by authoritarian regimes who are comfortable diverging from established rules.

Threats to national security are more diverse, emanating from a diffusion of actors who are enabled by technology. Actors who can wield an array of means and ways to further their security interests at the expense of a target, and are able to do so without being detected or crossing any clear threshold of response.

The concept of hybrid threats has been one response to these challenges. While often criticised for being a nebulous and contested idea, it still provides a useful framework to interrogate the contemporary security environment and new methods employed by competing states. The 'hybrid' label is often used interchangeably with others such as 'sub-threshold' and 'grey zone' but the characteristics of the underlying phenomena remain the same: adversaries combining and synchronising different measures to achieve strategic objectives, while remaining below the threshold of open conflict. Ultimately, these measures are about influencing political leaders and the decisions they make. This is why the subject is of interest to those in the field of Strategic Communications.

COMMUNICATIONS AS STRATEGY

People make decisions based on their social conditioning, experience and cognitive biases. They see the world around them and interpret events based on their own perception, whether this is through direct experience (I can see it is raining outside so I will need an umbrella) or via mediated channels (the weather forecast says it is raining so I will need an umbrella). This perception becomes their reality. This 'reality' where people understand the world around them and make sense of what it

means is described by the concept of the *information environment*. This is a model which can be used to understand how different audiences - publics, stakeholders and political leaders - are influenced to make decisions.

It is accepted that states seek to influence other actors, whether they be friendly, hostile or neutral. Influence is all about communication. When a state acts to influence another state, it is usually based on an assumption made by the political leadership – that their actions will communicate something that will achieve a preferred outcome. Technology has altered the dynamics of this interaction. Changes in speed, cost and access dictate that information is no longer transmitted at the speed of matter but at the speed of light. Governments must adapt with new methods and structures to address these challenges. The Strategic Communications mindset seeks to accommodate these changes in the character of geopolitical competition. It provides coherence to strategic influence by striving to understand how audiences see the world and then ensuring that planning is integrated and plans are executed with consistency. This is not communication *of* strategy but communication *as* strategy.

2. METHODOLOGY

The research has two aims. First, to exploit the data from our previous report,[2] developing *ways of looking* at hybrid threats. It explores the array of hostile measures and narratives used by states, giving an idea of where to look when detecting and identifying threats. Second, to *demonstrate* how the principles of Strategic Communications might be applied at the national level. This means understanding audiences and their information environment, then developing a strategic narrative in order to facilitate a coherent, inter-agency approach to strategic influence.

Our first report analysed thirty case studies providing examples of hostile measures that fit the hybrid description. From a list of 250, the cases were categorised into 14 thematic areas of threat. 30 case studies were chosen as a cross section sample of those thematic areas. Each case study identified key actors, the different measures they combined to leverage influence and the vulnerabilities of the targeted states they sought to exploit.

In this report analysis has been broadened to include audiences and narratives. Patterns and trends have been identified by comparing data across the case studies.

Case studies used for the research

	Case Study	Thematic Area
1	Russian snap exercises in the High North	Coercion through threat or use of force
2	Confucius Institutes	Government Organised Non-Government Organisations (GONGO)
3	2007 cyber attacks on Estonia	Cyber operations
4	US Transit Center at Manas	Economic leverage
5	The spread of Salafism in Egypt	Political actors
6	Disinformation in Sweden	Media
7	Hamas' use of human shields in Gaza	Lawfare
8	The 2010 Senkaku crisis	Economic leverage
9	Humanitarian aid in the Russo-Georgian conflict	Lawfare
10	Chinese public diplomacy in Taiwan	Exploitation of ethnic or cultural identities
11	Detention of Eston Kohver	Espionage and infiltration
12	Finnish airspace violations	Territorial violation
13	South Stream pipeline	Energy dependency
14	Russian language referendum in Latvia	Exploitation of ethnic or cultural Identities
15	Institute of Democracy and Cooperation	Academic Groups; NGOs; GONGOs
16	Zambian elections 2006	Economic leverage; Political actors
17	Serbian Orthodox Church	Religious groups
18	Communist Party of Bohemia and Moravia	Political actors
19	Bronze night riots	Exploitation of ethnic or cultural identities / Agitation and civil unrest
20	Russiky Mir Foundation in the Baltics	Government Organised Non-Government Organisations (GONGO)
21	Criminal networks in the Donbas	Bribery and corruption
22	Civil disorder in Bahrain 2011	Agitation and civil unrest
23	Pakistani involvement in Yemen	Economic leverage
24	Operation Parakram	Coercion through threat or use of force
25	Snap exercises and Crimea	Coercion through threat or use of force
26	Electronic warfare during Zapad 2017	Territorial violation
27	Russian espionage in Sweden	Espionage and infiltration
28	Religious extremism in the Netherlands	Exploitation of ethnic cultural identities
29	Cyber attacks on ROK & US	Cyber operations
30	Casas del ALBA in Peru	NGO

> Hybrid threats target vulnerabilities - systemic weaknesses in a nation. Adversaries are aware of these vulnerabilities and may probe them to exploit at later date.

3. THE HYBRID THREAT ENVIRONMENT

Despite the controversy which surrounds the term 'hybrid', it remains a useful umbrella to describe, without necessarily defining, a basic concept: that hostile states can combine and synchronise different instruments of power, furthering their strategic aims while remaining below the threshold of open conflict.[3] The specificity of hybrid threats can be distilled into two key characteristics: the **integration of measures** and **ambiguity.**

INTEGRATION OF MEASURES

State actors have a range of means available, their **instruments of power**, to leverage influence within the international system. Hybrid threats involve a combination of these means and their employment, hence the hybridity. Malign actors blend these instruments together, employing them asymmetrically and matching their strengths against any weakness of a targeted state. Such measures exploit vulnerabilities at all levels (national, regional and local) of the political system within a targeted nation. They aim to influence decision-making to further their own strategic objectives.

The instruments of power are traditionally broken down into Diplomatic, Information, Military and Economic (DIME).[4] NATO's crisis response planning tool refers to Military, Political, Economic, Civilian and Informational (MPECI).[5] Other studies have expanded this even further to thirteen 'domains'.[6] In the context of hybrid threats, NATO uses the expanded US model, including Financial, Intelligence and Legal to create DIMEFIL. This is the framework used for our analysis.[7,8]

AMBIGUITY

The actor responsible for any hostile measure, their intent and means employed may be deliberately obscured. If challenged, an actor can plausibly deny involvement. This lack of clarity makes detection, identification and attribution of threats a significant challenge. The first steps are to identify who might be responsible and if their actions have hostile intent.

It is expected that states will compete over interests. If an actor, however, is working to further its own strategic objectives at the expense of a target nation's security, competition becomes hostility and a threat to national security interests. This is not warfare in the sense that it involves the direct application of military power, but follows the logic of war, a zero-sum game where there is a winner and a loser, instead of cooperation from which both sides benefit.[9] The blurred boundaries between cooperation and competition creates ambiguity, making it difficult to identify the difference between actions which could be mutually beneficial or cooperative, and those deemed to be damaging to national security interests. This area of ambiguity between cooperation and competition, or between peace, crisis and war is sometimes referred to as the 'grey zone'.

Identification of any activity as hostile is based on threat assessments and ultimately a political decision by the government of the targeted nation. There may be no 'smoking gun' and public opinion may need convincing credible and compelling evidence. The qualification of 'hostile intent' is the most important factor to define and identifying an act as hostile is known as **attribution**. Actors responsible for hostile measures may be employed directly by a source nation, acting on their behalf, or working independently in a manner which supports an adversary's interests. An example is cyber-attacks where the perpetrator of a hack may be employed directly by the state, an organisation funded by the state or may be ideologically inspired to act in a manner aligned with the state's interests, either intentionally, or through self-interest such as criminals.

Persistent competition between states creates a challenge for threat assessment and the planning process, both of which must be *initiated* under certain circumstances. Planning is designed to enable the transformation of unacceptable conditions into acceptable conditions. If it is not possible to identify unacceptable conditions or initiate planning in a timely manner then responses to sub-threshold threats may not occur until it is too late. Governments therefore need the ability to *horizon scan* continuously, understanding actors and their interests, and identifying emerging threats and hostile measures before they can cause damage. States also require extant baseline or contingency plans which do not rely on a crisis response to be initiated.

Hybrid threats **target vulnerabilities**, systemic weaknesses in a nation. Adversaries are aware of these vulnerabilities and may probe them to exploit at later date. Institutional weakness in applying the principles of Strategic Communications can be a vulnerability, as can public trust in the ruling authority.

Analysis of the case studies identified 13 key types of hybrid threat. These involve a combination of measures, occurring in

Type of hybrid threat	Strategic logic
Direct influence of public opinion	- Establishing, funding or supporting academic, educational or cultural institutions. - Misinformation; fake news or disinformation campaigns. - Setting up or supporting media and news channels; media ownerships and advertisement campaigns; pressuring journalists.
Exacerbation of societal divisions	- Funding, supporting or promoting national, religious or political extremist organisations. - Polarisation of political debates to subvert a specific policy programme. - Exploitation of ethnic or cultural identities to undermine social cohesion.
Agitation and civil unrest	- Agitation of a targeted societal, cultural, religious or ethnic group to call for policy change or to initiate protests in targeted nation. - Disruption of political or economic processes through protests or boycotts. - Risk of radicalisation or violent escalation.
Interference in elections	- Foreign interference in elections to influence the voting behaviour of the population.
Decreasing public trust in government	- Decreasing public trust in government and military; discredit target government and public institutions. - Undermine credibility and legitimacy of policies and operations. - Creation of public insecurity; bribery and corruption scandals; blackmail and extortion.
Undermining governance and state functions	- Foreign state sponsoring of a political party or actor. - Corruption and criminal networks, organised crime. - Establishment of parallel informal government structures through information, education and healthcare systems.

Type of hybrid threat	Strategic logic
Diplomatic pressure	- Decrease diplomatic and domestic scope of action of target government through pressure, threat of use of force, intimidation or coercion; exacerbate dependencies. - Discredit government to damage international reputation, deteriorating relationship with international partners and allies. - Risk to become platform for proxy conflict; regional instability.
Economic leverage	- Economic pressure; economic or energy dependency; use of sanctions or incentives; disruption of business operations. - Extraction of valuable resources from disputed territories. - Marginalisation of local work force; creating informal working conditions for local workers in the source nation creating health and safety risks. - Exacerbate or create economic disparities and weak economy (Uneven regional development, social inequality, poverty).
Cyber operations	- Disruption of communication flows and other digital infrastructure. - Cyber-attacks as statement of intent and capability. - Psychological effect on citizens and investors; public insecurity and decreasing trust, political embarrassment.
Terrorism & violent extremism	- National, religious and political extremism. - Risk of domestic terrorism; resurgence of former terrorist organisations. - Ethnically motivated acts of violence; escalation of socio-political protests; sectarian violence.
Espionage	- Financial, physical, security-related, and reputational losses associated with espionage activities; decreasing public trust. - Corporate, cyber and political espionage.
Territorial disputes	- Regional instability; spill over effects on other territorial disputes; separatist regions within state borders. - Strengthened separatist movements.

A brief history of Hybrid Threats

The idea of hybridity has evolved alongside those conflicts it has described and which have provided empirical evidence.[10] The first appearance of the term is in Nemeth's 2002 study, 'Future War and Chechnya: A case for hybrid warfare' which referred to the idea of hybrid military forces, focusing on a blend of new technology and unconventional tactics. Building on Nemeth's concept, Hoffman goes on to describe Hezbollah's forces strategy against Israel in 2006 as a cross between an army and a guerrilla force.[11]

In 2009, in the context of ongoing operations in Afghanistan and Iraq, US Secretary of Defense Robert Gates said that he expected that "complex hybrid warfare" would become increasingly common. America's dominance with conventional military capabilities would give incentives to adversaries to use asymmetric means to exploit its strengths and undermine weaknesses.[12] The U.S. Department of Defense (DoD) saw two different aspects to this threat, irregular warfare with combatants blending in 'among the people' using suicide attacks and roadside bombs, and 'high end' asymmetric tactics employed by 'rising regional powers' and 'rogue states' using sophisticated technology for tactics such as anti-satellite, anti-air, anti-ship capabilities, weapons of mass destruction and cyber capabilities.

The US DoD 2010 Quadrennial Defense review tentatively introduced the idea, reporting that the "term 'hybrid' has recently been used to capture the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. These may involve state adversaries that employ protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states."[13]

Hybrid threats enter NATO's lexicon in 2010, initially defining them as "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives".[14] This was in the context of "the interconnectedness of the globalised environment", facilitated by rapid technological change which had enabled an increase in the speed, scale and intensity of attacks.[15]

Arguably, the most influential reference point for NATO and the nations is the start of Russia's ongoing actions in Ukraine in 2014, which has become the archetypal example of hybrid 'warfare'.[16] The concept of hybrid warfare in this context expanded beyond focusing on the use of predominantly military instruments to include political, economic and social systems.

In 2016, the European Commission published their framework on countering hybrid threats, describing "the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-

making processes." [17,18]

The NATO Brussels communique in 2018 highlighted that "Our nations have come under increasing challenge from both state and non-state actors who use hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict." This was recommitted at the 2019 London leaders' meeting with Jens Stoltenberg saying NATO needed to step up its response to hybrid threats.[19]

In 2020 the European Centre for Countering Hybrid Threats published a model to describe the landscape of hybrid threats, describing them "as old as conflict and warfare, repackaged and empowered by changing security environment dynamics, new tools, concepts and technologies, targeting vulnerabilities" with the aim of "undermining public trust in democratic institutions, deepening unhealthy polarization [..] challenging the core values of democratic societies, gaining geopolitical influence and power through harming and undermining others, and affecting the decision-making capability of political leaders".[20]

> The information environment is a conceptual space which helps us describe how audiences perceive the world, deduce meaning from it and how that affects their attitudes, decision-making and behaviour.

4. STRATEGIC COMMUNICATIONS

At the heart of NATO's approach to Strategic Communications is an appreciation that 'everything communicates'.[21] What we say or do (or do *not* say or do) sends a message. Actions, words and images communicate with audiences, influencing their perceptions and decision-making. This applies to strategic effects such as deterrence, compellence, coercion and reassurance. These are ultimately resolved in the minds (or *cognitive dimension*) of any adversary, ally or stakeholder in the international system. Part of the StratCom process is understanding the dynamics of this decision-making through the lens of the information environment.

For this report we adopt a generic definition of Strategic Communications as:

"An approach to communication, based on values and interests, that encompasses everything we do or say to achieve objectives in a contested environment".[22,23]

When this approach is applied, Strategic Communications takes political direction and articulates it - along with objectives - in the form of a strategic narrative. This narrative describes the trajectory of how we see events playing out to our advantage. It is then is then used to ensure actions across the entirety of an organisation are coherent and it projects the desired image. There is

nothing revolutionary about using different instruments to send 'messages' and 'signals' (see table p16). When politicians talk in this way, they are already adopting the Strategic Communications approach, although they might not call it that. When StratCom is applied effectively as a function, it increases the likelihood of the right signal being communicated to the right audience at the right time.

Communication is therefore not be something to be considered once a strategy has been developed and requires a communication or information strategy to support it. The communicative aspects of potential courses of action should be factored in from the start. Some actions will not be taken with the explicit intent of communicating (e.g. logistics or trade agreements) but will still impact the information environment. Other actions will have the sole intent of sending a message (e.g. sanctions or the expulsion of diplomats). The big idea behind Strategic Communications is that *all* of these activities are integrated in a coherent way.

The extent to which any state can influence other states or actors to engage in political change is based on a combination of different instruments of power.[24] The relationship between the 'information' instrument and other instruments of power is conceptually unclear. The elements of instruments of power are indivisible and none can exist in the absence of another, however there will be only one strategic narrative, although this may change over time.[25] Capabilities such as international broadcasting or public diplomacy could be considered as discrete informational instruments but information also enables, and is a product of, the other instruments of power.

Information should therefore be considered across the entirety of strategic thinking, not just as a separate instrument. A successful national strategy appreciates that there is an informational dimension to every instrument of power, integrating different tools to influence decision making. This is often referred to as the 'Whole-of-Government' (W-o-G) approach.

In this context, information is the pervasive, intangible cloud of stimuli that surrounds people, their *information environment*. Whether perceived through direct observation, conversation, social media or television and radio, information provides the currency for communication. It forms the basis for people to deduce meaning from the world around them, form opinions and make decisions.[26] Communication is the creation and conveyance of meaning based on the perception of the human mind and how it processes information.

Understanding the dynamics of information and communication means striving to understand the information environment. This information environment is not a place where activity takes place or a physical domain with boundaries such as land, sea or air. It is a conceptual space which helps to describe how audiences perceive the world, deduce meaning from it and how that affects attitudes, decision-making and behaviour. Understanding the information environment therefore requires a persistent, systematic analysis of relevant actors and audiences, plus identification of the different methods and narratives used by adversaries.

States routinely use different measures to send 'messages' and 'signals'. As a function, Strategic Communications increases the likelihood of these actions achieving desired outcomes.

Activity	Target audiences	Measures
"The US sending two carrier strike groups to the Mediterranean Sea will **demonstrate capability** to Russia"[27]	**Adversary** Russian government	Information, Military
"Finland and Sweden conducting a joint exercise to prepare for information influence activities will **reassure home populations"**[28]	**Adversary** Russian government **Domestic** Home populations	Information, Military, Legal (law enforcement)
"The US **sending troops and military equipment** to Saudi Arabia will **reassure** Saudi Arabia and alarm Iran"[29]	**Adversary** Iran **Allies** Saudi Arabia	Information, Military
"Indonesia **deploying fight jets and warships** to patrol Natuna Islands will **deter** Chinese vessels"[30]	**Adversary** China	Information, Military
"Latvia, Estonia and Finland **launching a joint gas market** will **demonstrate** 'energy independence' to Russia"[31]	**Adversary** Russia	Information, Economic
The US **testing interoperability** with NATO allied forces and partners will **reassure Alliance members** and partners[32]	**Adversary** Russia **Allies** NATO alliance members and partner forces	Information, Military
The UK **investing £36 million in cyber-security projects** will **reassure** domestic businesses and deter potential cyber-criminals	**Domestic** Population	Information, Military, Legal (law enforcement)
Estonia **asserting the right of collective defence** in cyberspace will **alarm** state-sponsored cyber-attackers	**Allies / Friendly** International community **Adversary** State-sponsored cyber-attackers	Information, Military, Legal (law enforcement)
The US **supporting anti-corruption efforts** in Ukraine will **reassure** the Ukrainian population[33]	**Allies / Friendly** Ukrainian population **Adversary** Russia	Information, Financial
The US **conducting more patrols** in the South China Seas will **warn** China to "abide by international rules"[34]	**Adversary** China	Information, Military
The UK and 28 other countries expelling over 150 Russian intelligence officers **demonstrates** "collective solidarity" to Russia [35]	**Adversary** Russia	Diplomatic, Information, Intelligence.

THE PRINCIPLES OF NATO STRATEGIC COMMUNICATIONS [36]

The NATO StratCom principles remain relevant at the national level.

Words must match actions. The 'say-do' gap occurs when what is said does not match what is done (and vice versa). When organisations and governments let this happen it erodes credibility and trust.

The information environment must be understood. The information environment is a model which helps us understand how people experience their 'reality' and the meaning they interpret from it. This means understanding the different ways in which humans deduce meaning from their own personal experience and how this affects the decisions they make.

All activity is founded on values. Nations should not act in a way which contradicts their stated values, such as by undermining a declared adherence to rule of law, human rights and equality.

Actions should support an objective, derived from policy and strategy and aligned with political direction. Political guidance forms the basis of a strategic narrative which outlines the government's overall approach to a security issue. Having a narrative ensures a common understanding of the problem and enables unity of effort through inter-agency cooperation.

Credibility and trust are vital resources. Credibility is the cornerstone of strategic influence, especially deterrence. Trust is the glue that allows international cooperation to take place, coalitions to be formed and conflict to be resolved.

Communication is a collective and integrated effort. 'Communicating' is not the sole responsibility of communications professionals. Every person within an organisation, the things that they say, actions they take and policies they develop will communicate something. The more coherent this process is within an overarching narrative; the more unity of effort is achieved.

Focus on effects and outcomes. Actions should be planned to influence audiences, for a purpose.

Communication is empowered at all levels. Government branches should understand what the 'big idea' is that underpins all activity. Clear direction and guidance should be given that allows mission command to take place.

5. UNDERSTANDING

A threat is the *perception* of some degree of danger based on an assessment of any given situation, which considers both our own and the adversary's capabilities, intent and objectives.[37] It is therefore a subjective assessment of the rationale which lies behind activities suspected as targeting a nation. This assessment requires an in-depth appreciation of the information environment and will draw insights from many different sources. It is unlikely that there will be clear, black and white assessments of threat.

Measures used by adversaries in the grey zone can be difficult to identify or predict.[38] Identifying hybrid threats relies on 'joining the dots' between different indicators and assessing when competition crosses a threshold to become unacceptably hostile. This means continually monitoring known actors of interest but also looking for 'unknown unknowns', those things we are neither aware of nor understand.

Looking for potential threats requires **horizon scanning**, an interdisciplinary and systematic search, informed by security requirements and strategic intent, for potential threats and opportunities.[39] Intelligence collection and analysis is often limited to specific instruments and tends to focus on smaller pieces of the jigsaw.

The aim of horizon scanning is to develop situational awareness, identifying trends and linkages over time, and relating these to what is happening (or not happening).[40] In addition to understanding the different measures being employed, *strategic logic* is a way of attempting to understand the underlying rationale behind an actor's behaviour - what they are doing and why.

Ambiguity means that identifying the threshold between acceptable and unacceptable behaviour can be a challenge. Persistent monitoring of indicators in the threat landscape can support the development and monitoring of thresholds.

This requires an understanding of relevant **actors**, their **strategic objectives**, the **measures** they employ and which of our own **vulnerabilities** might be exploited. All of these are wrapped up in the **narratives** adopted by any hostile actor, designed to target different **audiences.**

6. ACTORS

Actors are persons, organisations, groups or societies, including state and non-state entities,[41] within the international system that have the capability or desire to influence others in pursuit of their interests. Actors are relevant if their behaviour is likely to have a significant impact on the achievement of national security objectives. Viewed through the lens of the information environment, actors need to be set in their cultural, institutional, technological and physical context. This helps develop a better understanding of their motivations, perceptions and the decisions they make.[42]

There is likely to be a diffusion of actors working to further the interests of any hostile state. Such actors may be *assets*, under direct control of the state (e.g. state-owned business enterprises or the military), *supported* by the state, such as through funding or training (e.g. GONGOs) or *inspired* by a state's ideology (such as though language, religion or identity). The actor responsible for hostile measures and their intent may be challenging to identify, particularly when different actors and measures are used to create synergistic effects over time.

Analysis of the case studies identifies the following categories of significant actors which should be the primary focus when developing an understanding of the threat landscape.

- **Hostile state**. The state assessed as responsible for the threat or hostile measure;
- **Targeted state**. The state being targeted by the threat or hostile measure;
- **Stakeholders**. Other states that are involved in the interaction. Third party actors often have a strong preference for specific outcomes, shaping events according to their own interests. This can either mean supporting the source or target nation or functioning as a mediator to de-escalate the situation;
- **International Organisations (IOs).** IOs, such as EU and NATO, are involved in cases where hybrid threats target their member states or allies, or impact security interests of the IO. The threat evaluation of IOs often differs from the target nation's assessment.
- **Unknown**. When it is not possible to identify the actor responsible for a specific measure.

The following **sub-state actors** were identified as being significant:

- **Political**. Government agencies, head of states, political parties, opposition politicians, individual high-ranking public figures, diplomats, embassy staff;
- **Military and security**. Intelligence services, agents, regular troops, irregular/ paramilitary troops, individual high-ranking officials;
- **Civil society**. Universities, think tanks, academics, celebrity influencers, NGOs, religious groups, charitable organisations;
- **Economic**. Financial institutions such as banks, state-owned and private corporations.

7. HOSTILE NARRATIVE STRATEGIES

Strategic narratives are a representation of events and actors, used as a communicative tool through which political leaders give determined meaning to the past, present and future to achieve political objectives.[43] Actors have a preferred narrative which is likely to be at odds with that of a competitor. It will be based on factors such as political discourse, history, cultural norms and national security strategies. Strategic narratives encapsulate a state's identity and why it behaves as it does.

Analysis of narratives suggests that the most common strategy is for a hostile state to frame a set of circumstances as being a threat, to which they are obliged to respond. They then justify this response using legal or ethical reasons.

Prevalence of narratives in case studies

According to analysis of the case studies, narratives constructed by hostile states can be categorised into the following themes, as they attempt to frame the discourse around events in a manner favourable to their interests.

- **International order and ethics.** Narratives which aim to legitimise actions based on international law and ethical notions of right and wrong, for instance by referring to commonly accepted norms, such as multilateral conflict resolution.

- **Governance and human rights.** Narratives framing hostile measures in terms of a responsibility to protect foreign citizens against the failure of their government.
- **Identity and culture.** Narratives which aim at creating a transnational community based on religion, language, culture, or ethics. This provides the basis for legitimate involvement as the source and target nation are portrayed as one in-group.
- **Economics.** Narratives aimed at normalising actions as ongoing economic competition, or as creating dependencies, by persuading the target nation of the benefits that come along with enhanced trade relationships, economic assistance or development aid.
- **Security, war & military** Messages intended to frame actions in terms of defence; routine exercises or safeguarding national security and regional stability.

Hostile states combine different strategies to influence key audiences, attempting to construct narratives that are resonant and effective. Narratives can either be **proactive** or **reactive**.

- **Proactive** narratives are based on values and build on strong notions of justice and legitimacy, referring to human rights or international law. The narrative is constructed according to several steps that combine positive and negative positions. A hostile state presents a situation as threatening with a legal or ethical justification to respond, then attributes responsibility of the threat to another actor. The state then attempts to establish a transnational community based on a common identity such as religion, ethnicity or language. It then eventually presents a solution, often portrayed as the only option or an ethical necessity.
- **Defensive** strategies create ambiguity and plausible deniability by normalising events as being the status quo or by denying involvement.

8. CRITICAL FUNCTIONS AND VULNERABILITIES

Assessing where a hostile state can damage national security interests means deciding what needs protecting - **critical functions** - and where the weak points are, **vulnerabilities**.

Critical functions are functions which are so vitally important to a nation's wellbeing that they must be protected or sustained. If these functions are affected, it could lead to a disruption of a nation and its society. Critical functions can be broken down into a combination of processes (e.g. legal, technical, political) and infrastructure (e.g. power grids, healthcare).[44]

Analysis of the case studies identified five broad areas of critical functions: **governance and democracy**; **society**; **media and public information**; **economics**; **defence and security**; **diplomacy and geopolitics** and **infrastructure**. Critical functions are usually referenced in national security strategies.

What are we trying to protect? (Critical functions)

Governance & Democracy

- Sovereign political decision-making; free democratic debate; strong civil society.
- Trust in democratic institutions and processes; perception of political stability and good governance; government credibility; transparency.
- Free, fair and independent elections; diverse and functioning political parties.
- Rule of law; functioning legal institutions; civil rights; constitutional order.
- Control over state territories and borders; reintegration of disputed territories.
- Government control and emergency management capacity; control over classified information.

Society

- Social cohesion and unity.
- Positive and inclusive national identity.
- Integration of different ethnic, cultural, political and religious groups.
- Public trust in and support of military, legal, political and media institutions.
- Diverse and strong civil society;
- Working welfare state and health systems.
- Functioning education systems and academia.

What are we trying to protect? (Critical functions)

Media & Public Information

- Functioning, diverse and balanced media landscape; freedom of press; professional journalism.
- High level of media literacy; public trust in mainstream media outlets.
- Informed and balanced public debates; resilience against disinformation.
- Public trust in government communications, spokespersons and official channels.
- Sovereignty of the information environment
- Control over classified information, public databases and records.

Economics

- Sustainable economic development and stability.
- Protection against industrial espionage.
- Reliable financial institutions and infrastructure.
- Economic independence and cooperation with partner states.
- Energy security.
- Welfare state, low rate of unemployment, poverty and inequalities.

Defense & Security

- Domestic security; low risk of terrorism and violent extremism; regional stability.
- Safe living conditions and public perception of security.
- Functioning military troops and equipment; effective defence; capability development.
- Defence cooperation.
- Territorial integrity; border security.

Diplomacy & Geopolitics

- Strong bi- and multilateral alliances with partner states (political, economic, military) and IOs.
- International law, norms and institutions.
- Positive reputation and image; value-based nation branding.
- Regional stability; balancing of regional competitors; safeguarding interests over disputed territories.
- Economic and energy independence.

Infrastructure

- Safety of information systems, national databases and registries; internet; civil communications systems and related emergency networks.
- Safety of transportation systems on land, air and water, including energy and fuel supply.
- Power plants, water supply, energy transmission, pipelines.

A **vulnerability** is a weakness or gap in national security, usually related to a critical function. They can be exploited by an adversary.[45] Any factor associated with a weakness in the critical function of a nation may be considered a vulnerability, which can be anything from lack of public trust in the government to a high reliance on technology.

Analysis of our case studies mapped the vulnerabilities associated with critical functions. Many of the competencies responsible for mapping vulnerabilities lie with different government ministries, so an inter-agency approach is required when understanding where there may be weaknesses.

Where are the weak points? (Vulnerabilities)

Governance & Democracy

- Corruption of political elites, security services or law enforcement (salaries, funding).
- Infiltration or cooperation of political elites with source nation.
- Weak state institutions; lack of political will; poor governance; tradition of clientelism between government and business.
- Lack of transparency and accountability; lack of public trust.
- Political cleavages and extremist parties; polarised debates and pre-existing political-ideological divisions.
- Legal loopholes; limits of law enforcement.

Society

- Societal cleavages, tensions between different ethnic, religious, political, cultural or other identity groups.
- Failure to integrate minority groups.
- Polarised debates and pre-existing ideological divisions.
- Weak civil society.
- Lack of funding for educational, academic or charity organisations.
- Inequality and poverty, lack of public healthcare, infrastructure and education.

Where are the weak points? (Vulnerabilities)

Economics

- Economic dependency; dependency on importing resources, energy or on humanitarian/economic aid and investment.
- Energy dependency or shortage
- Lack of funding and resources for public institutions (security and defence, education; healthcare etc.)
- Poverty and unemployment; dependency on importing resources, energy or on humanitarian/economic aid and investment
- Weak economy; debt and weak currency.

9. AUDIENCES

An **audience** is a group of people or an individual with similar opportunities of being influenced by actors. Identifying audiences is a way of categorising actors, ensuring planning generates the most appropriate activity to communicate with the right audiences. Analysis of our case studies identified particular audiences as reappearing in many of the scenarios**.** This does not mean that other audiences are not be relevant but provides an indication of where the initial focus of analysis should be.

At the highest level, audience segmentation is simplistic but allows for further analysis to identify subset audiences of specific interest. The first categorisation of actors is into those who are **allies**, those who are **hostile** and those who are **uncommitted** or **neutral**. When more detailed planning takes place, audiences can be further segmented based on location, race, gender, ethnicity. status, beliefs, values and identity.[46] The categorisation and research of audiences is achieved through a process called **audience insight** [47] or **target audience analysis**.

Common audiences in hybrid threat scenarios

Hostile	Friendly	Uncommitted / Neutral
Affiliated Government-Organised Non-Government Organisations	Political party supportive of targeted state	Language specific media outlets
Affiliated Non-Government Organisations	Targeted state's domestic population	International Organisations
Adversary political leadership	Intergovernmental organisations connected to target nation	
Affiliated nation minority in target nation	Target nation military leadership	
Political party supportive of hostile state	Political leadership supportive of hostile state	
Media outlets affiliated to hostile state's political leadership	Political leadership supportive of targeted state	
Domestic population of hostile state	Individuals within target state political leadership	
Energy actors affiliated to hostile state's political leadership		
Religious groups supportive of hostile state		
Supporters of political party affiliated to hostile state		
Hostile nation's military leadership		

10. HOSTILE MEASURES

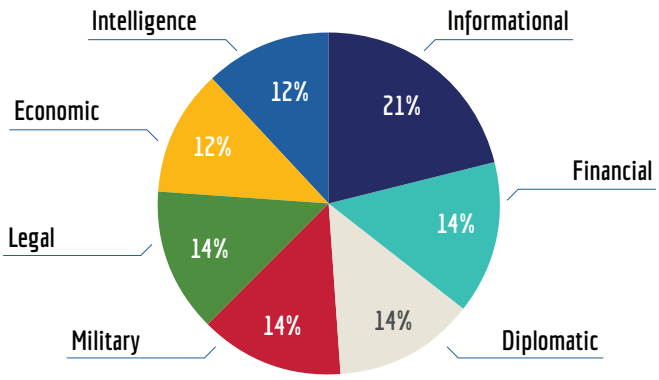
A measure becomes hostile when it passes a certain threshold to inflict damage on the national security of a targeted state. This threshold (or *red line*) is the point at which a government decides an activity has gone beyond an acceptable level of competition, demanding a response. It is not practical for governments to respond to every potential threat, so thresholds must be set according to what level of hostility can be reasonably tolerated and under what circumstances a response is required.[48] Thresholds are often subjective, based on different interpretations of events by different audiences. They are therefore 'elastic' in the information environment and can be manipulated by the actor responsible as context changes over time. This flexibility can afford the hostile actor freedom of action to inflict damage without provoking a response from the targeted nation. Being agile enough to act swiftly based on changes in the information environment can reduce an adversary's potential courses of action.

When an actor is identified as being responsible for a hostile measure, this is called **attribution**. The ability and willingness to attribute effectively is an important part of deterrence and is most effective when done as part of a coherent response taken with allies. Attribution is a political endeavour often based on intelligence that cannot be released in its entirety. Audiences are likely to demand evidence that is **credible and compelling** before they trust any government's assessment.

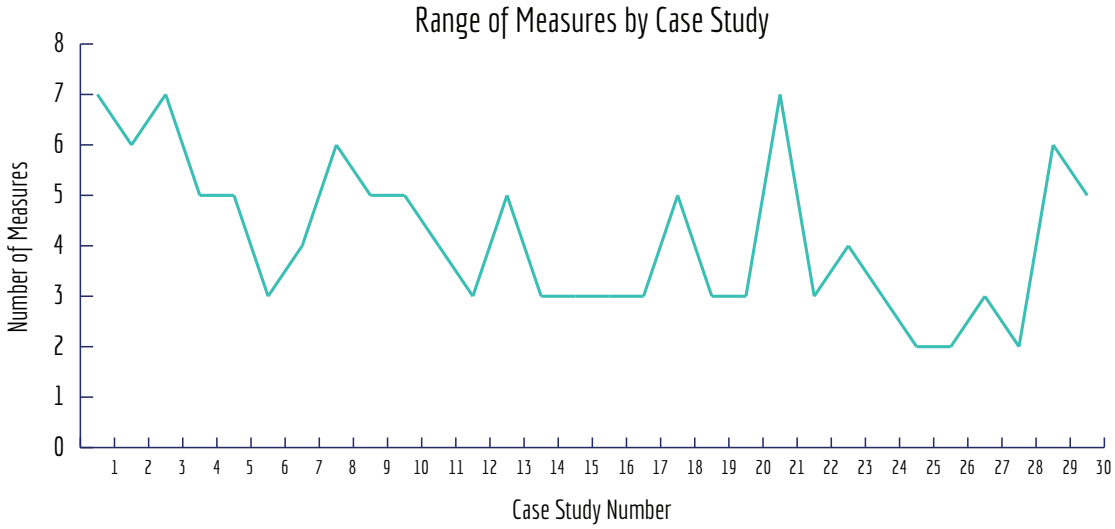
In analysis of the hostile measures employed by states, at least 2 instruments of power were employed in all cases. In 3 cases (1, 3, 21) the source nation employed all 7 instruments of power. In these cases the Russian Federation was identified as the hostile state, indicating their high capability to resort to a wide range of measures in their hybrid activities. In case studies 2, 8 and 29, 6 different instruments were used (2 and 8: China, 20, DRNK).

The most common measure identified in the case studies was **information**, employed in 25 of the 30 cases analysed. Other instruments were observed in about half of the cases.

Prevalence of measures used in studies



Each case study has a combination of measures, with never less than two being involved.



The following sections are from comparative analysis of the different measures identified in the case studies, broken down into DIMEFIL categories.

DIPLOMATIC MEASURES

Diplomacy is the principal instrument a nation uses for engaging with states and foreign groups, advancing values, interests and objectives, and soliciting foreign support.[49]

In the case studies, **public statements** by high-level government officials are the most common observable diplomatic measure, featuring in 17 out of 30 of the scenarios. These statements can be **negative**, such as criticism, disapproval or warning, or **positive** such as showing support.

The strategic logic behind diplomatic measures falls into three categories: **negative**, ranging from coercion and delegitimisation to agitation and infiltration; **positive,** aimed at gathering support or claiming legitimacy; or **neutral**, denying involvement or trying to create plausible deniability.

States use bilateral diplomatic channels to leverage influence. They also play **two-level games**, where states negotiate simultaneously at both the *intranational* (domestic) and the *international* level. In these cases, International Organisations and other states are engaged to build-up international pressure.

Measure	Rationale
- Use of IOs or tribunals, (e.g. addressing the UN) - Alliances with partner states	- Two-level game - Legitimacy - Pressure - Lobby for sanctions or prosecution
- Diplomatic visits	- Pressure - Nation branding / public diplomacy - Support
- Ignoring or playing down an incident - Suspension of bilateral contacts	- Plausible deniability - Delegitimise - Non- recognition
- Influencing government officials or close advisors	- Infiltration
- Public statements (criticism, warning, or support)	- Agitation, pressure; discredit - Plausible deniability; downplaying the incident; sugar-coating - Nation branding; showing support
- Recalling diplomatic staff	- Pressure - No dialogue
- Expulsion of foreign diplomats - Summoning of Ambassador	- Pressure - Power demonstration

INFORMATION MEASURES[50]

Measures in this category tend to focus on dissemination channels for information and the intangible expression of soft power and cultural influence.

Education is the most common informational measure, covering the academic, religious, ideological and political realms. Measures can range from language and culture courses, building schools and organising conferences, to establishing Think Tanks. Educational measures are usually aimed at gathering support for a policy but can also stir up hatred, discredit the targeted government or agitate the population.

Hostile states can **establish** or buy up existing **media channels** to influence public opinion, including newspapers, radio and TV entities, often with targeted language and cultural content. Apart from media ownership, **media coverage** can be influenced through advertising campaigns, pressuring journalists or launching disinformation campaigns.

It is often difficult to identify the actor behind an informational measure. They create **plausible deniability** by establishing non-state and non-political institutions with opaque governance structures and financial arrangements.

Measure	Rationale
- Disinformation	- Discredit; polarise; weakening trust in government - Gather support - Create confusion
- Diplomatic visits	- Education (academic; religious; cultural; ideological; political) - Provide free literature - Support; legitimacy through academic objectivity - Discredit; polarise
- Establish, or purchase existing language specific media outlets	- Gather support; promote policy - Targeted outreach; creating language-based community - Discredit; polarise
- Media coverage; use of social media - Commercial advertising	- Dominate the narrative - Agitation - Support - Plausible deniability
- Disrupt communication between government and population	- Reputational damage
- Public events	- Support - Polarise

MILITARY MEASURES

The use of military capabilities generates effects through the direct application or threat of force, to compel or deter. The military also has capabilities that can be used in confrontations that are short of armed conflict.[51]

Readiness exercises or the **establishment of military bases** reassure the home population while pressuring or threatening competitors. Framed as purely defensive measures, source nations can draw on plausible deniability.

Indirect military measures such as the deployment or support (e.g. training, funding, supply of equipment) of irregular forces as well as awarding military equipment contracts are often difficult to detect or identify as hostile.

Measure	Rationale
- Military equipment contracts - Illicit arms trade	- Plausible deniability (proxies instead of official troops)
- Establish military bases	- Deterrence - Power demonstration - Plausible deniability (defence)
- Military force within civilian areas (e.g. launching of rockets)	- Asymmetric warfare - Provoke civilian casualties (pressure; decrease public trust)
- Airspace and territorial violations	- Control the narrative - Agitation - Support - Plausible deniability
- Threat of force	- Reputational damage
- Deterrence - Coercion - Demonstration of power	- Support - Polarise
- Readiness exercises - Testing military capabilities (e.g. rockets)	- Deterrence - Power demonstration - Defence - Pressure

ECONOMIC MEASURES

The use of economic inputs and flows to influence decision making.[52]

Economic measures can be either **negative** based on punishing sanctions, or **positive**, based on cooperation and investment.

Measures aimed at **creating pressure** include export restrictions, extended border checks or the disruption of business operations.

Measures aimed at **providing incentives** include investments, credits and financial aid, economic integration projects or enhanced trade relationships.

Measure	Rationale
- Criminal networks; corruption	- Undermining state capacity and trust in government - Infiltration
- Restriction of export quotas; border checks; Disruption of shipments	- Coercion - Economic leverage - Plausible deniability - Creating uncertainty
- Disrupting business operations by calling for boycotts, blockades, or civil unrest	- Economic leverage - Creating uncertainty - Discrediting ruling authority and decreasing trust in government
- Suspension of bilateral economic initiatives	- Coercion
- Transport of equipment to a disputed territory	- Fait accompli
- Investments; credits and financial aid; economic integration; enhanced trade relationship; incentives for investments (sponsored workshops, subsidised housing, tax breaks, financial grants)	- Incentive - Create dependencies - Influence - Branding - Support
- Funding of political parties	- Infiltration
- Use of state-owned and private companies; government-backed environment to investors; shell operations	- Plausible deniability

FINANCIAL MEASURES

The control of the creation, flow, and access to 'stores of value' wields power. Although finance is generally an operation of real and virtual currency, anything that can serve as a medium of exchange provides those who accept the medium with a method of financial transaction.[53]

The most common financial measure is **funding of political, cultural or academic institutions** in the targeted state, such as political parties or think tanks. It is often difficult to trace the funding flow back to a state actor.

Hostile states can also **interfere** with their target's **financial markets**. This can be either disruptive, for instance through cyber-attacks targeting banks and other financial institutions or based on incentives by directly investing in or attracting investments. While disruptive measures are aimed at generating uncertainty, decreasing trust in government and pressuring competitors, investments are designed to gather support and create dependencies.

Measure	Rationale
- Funding and financial transaction from state sponsors to supportive actors	- Arm's length influence - Threat diffusion - Difficult to detect and attribute - Cost effective
- Direct funding	- Distort business decisions - Subvert legitimate financial process - Compromise credibility of individuals or organisations
- Investments and credits	- Difficult to attribute as hostile

INTELLIGENCE MEASURES

Intelligence provides the national leadership with the information needed to realise national goals and implement national security strategy. Planners use intelligence to identify an adversary's capabilities and vulnerabilities.[54]

Intelligence measures can be employed to **gather information** about political, economic or military processes in the target nation, in order to get an informational advantage. Espionage can take many forms, from cyber operations and industrial espionage to recruiting human sources.

A source nation can also try to **interfere with decision-making** processes by placing agents or recruiting personnel in influential public institutions.

Measure	Rationale
- Industrial espionage; Corporate espionage and illegal technology transfers	- Economic advantage
- Agitation to protest; agitation to sabotage critical infrastructure	- Coercion - Polarisation
- Kidnapping and unlawful detention	- Coercion - Create uncertainty - Plausible deniability
- Espionage; military intelligence gathering; reconnaissance to test resilience	- Reconnaissance to test resilience
- Infiltrating politics, academia and news media by placing intelligence agents or recruiting employees and figures	- Infiltration - Influence decision-making
- Cyber espionage	- Identifying vulnerabilities
- Infiltration of intelligence services	- Intelligence collection of target nation

LEGAL / LAW ENFORCEMENT MEASURES

The attitude of the population, degree of control provided by competing (non-state government) enforcers of law, and traditions of civic order are key components of the overall law enforcement environment. All these varying conditions will contribute to the degree of lawlessness in any given society.[55]

Legal measures are often designed to **exploit the ambiguity** surrounding hybrid threats by framing actions as legitimate. States can exploit legal loopholes and contradictions in international law to legitimise their actions.

Legal measures can target international law or domestic legal institutions of the targeted state to **undermine legal procedures**. The underlying rationale can range from avoiding prosecution of allies to creating incentives or legitimising academic or cultural institutions through legal frameworks.

Measure	Rationale
- Arbitrary interpretation of international law and agreements; exploitation legal loopholes and contradictions	- Legitimacy: broad interpretation to convey conformity with international law
- Arbitrary or fabricated legal charges	- Pressure - Demonstration of power
- Create legal frameworks	- Support - Create incentives - Legitimacy - Legally institutionalising influence
- Infiltration of legal institutions; bribery and corruption in law enforcement	- Influence legal procedures
- Legal status as NGOs or private institutions	- Plausible deniability
- Provoke lawbreaking	- Discredit; delegitimise competitor

11. COUNTERING THE THREAT

Deterring hybrid threats and denying their effects requires foresight and preparation, to safeguard the status quo from being transformed by adversaries to their favour. The character of hybrid threats – persistent and ambiguous - demands steady state baseline planning as a continuous effort, not just something initiated by crisis.

The activities of potential adversaries need to be detected and monitored, to be able to assess when competition between states escalates into something more serious. Concurrently, an adversary's ability to restrict our own freedom of action must be denied. Responses will involve a range of government measures. These need to be coordinated so that they communicate with - and influence – the right target audiences, without risking undesired 2nd or 3rd order effects.

The Strategic Communications approach in this context means understanding the information environment, considering what different response options might communicate to key audiences and then choosing the right blend of activities to influence them. The output of this process is direction and guidance, articulated in a **Strategic Communications framework**.[56]

This guidance increases the likelihood that a state's response to any threat is coherent, communicating with audiences in a way which creates desired effects and outcomes. It ensures that all activities, whether planned with the sole intent of communicating or undertaken for other reasons are 'cut from the same cloth'. The framework should therefore be endorsed by a central authority, with input from each branch of government, not just defence.

Framework issue areas. Frameworks can be written to address specific issues, regions or events, so will have a different focus.

- **Actor focused**. (e.g. Russia, China) A framework which outlines an approach to a specific actor, usually a nation-state, covering the full range of measures they are assessed to be using.
- **Actor-action focused**. (e.g. Russian military exercises, Chinese territorial violations). When the framework is developed to address specific measures employed by a specific actor.
- **Event focused**. Anticipating an event threatened or caused by hybrid measures, or applying contingent methods to an event fitting in a predefined threat scenario.
- **Issue focused**. When there are several similar measures assessed as coming from different actors. (e.g. disinformation, cyber-attacks or economic leverage).

The StratCom framework is not a communications strategy in the traditional sense. It provides overarching guidance, a *golden thread* of a strategic narrative. The formulation of the narrative enables integrated planning and consistent execution for actions at all levels. It articulates the themes which capture the image that the government wants to project through its actions, words and images. More on the narrative is covered in the next chapter.

The format of a StratCom framework is an evolution of an information strategy, intended to provide a 'wrapper' for everything that a government or organisation does and says. It is not a specific plan but a codification of political guidance which allows for further planning on all other levels of command. The framework will have to be updated regularly providing continuous and valid guidance across government. It should preferably be an easy-access 'plan on a page' as to what actions should be taken and how those actions should be framed, to ensure the right message is sent to the right audience.

Based on an understanding of the IE, response options from different government agencies responsible for respective instruments of power should be planned with specific outcomes in mind. The rationale behind response measures falls between two, overlapping categories:

- **Communicative or informational measures**. An activity with the primary purpose of influencing a target audience.[57] The simplest example of this is a press conference which is conducted with the express purpose of communicating. Other activities can send messages, such as sanctions, the expulsion of diplomats or changes in force posture.
- **Measures whose primary purpose is not communicative**. Actions which are not undertaken with the primary purpose of influencing target audience, such as training or the movement of supplied. Despite not being designed with the intent of communicating, such activities will be interpreted differently by audiences.

Based on analysis of the case studies, responses to hybrid threats fall into three broad categories.

No Reaction.

- The assessment of whether an activity is considered a threat is a political decision. Governments can choose to assess an activity as not being hostile, maintaining the status quo.
- Maintaining the status quo can lead to the normalisation of an activity over time.
- In certain circumstances, not responding denies the effect, potentially preventing 'reflexive control'

Increased awareness. Increased awareness can act as a deterrent effect as populations who are more of any

threat are more prepared to deal with hostile measures, building resilience and reducing vulnerabilities.

- Increased government awareness of new threats and capabilities of competitors, especially Cyber, Electronic warfare and disinformation.
- Awareness of vulnerabilities including societal cleavages; sensitive political topics that are exploited; economic, military or political dependencies.
- Recognition of the need to build resilience, address vulnerabilities and strengthen democratic institutions.
- Public and media attention to hostile state activity.

Active responses.

- Increased resources and efforts to counter espionage, cyber operations and disinformation; capability development; increased military spending; resilience building.
- Strengthening international cooperation, IOs and alliances.
- Promotion of more moderate alternatives to extremist narratives, closure of TV channels and news outlets that promote extremist positions and/or are funded by foreign state actors.
- Measures to enhance public media literacy, initiatives on countering disinformation and fake news, bursting filter bubbles, and source criticism.
- Monitoring, investigating, or closing NGOs, academic, cultural or social institutions that are funded or supported by foreign state actors.
- Revising government response and communication strategies on dealing with ambiguity and lack of evidence.
- Supply and energy diversifications strategies.
- Modernising border security.
- Launching anti-corruption programmes; transparency initiatives on funding and sponsoring of political parties and politicians.
- Investigation and prosecution of criminal networks.

12. THE STRATEGIC COMMUNICATIONS FRAMEWORK

Direction and guidance in the frameworks enable political guidance to be communicated internally and for execution to be devolved to the lowest level. This allows for a delegation of responsibility, in military culture called *mission command*. This is similar to the civilian concept of *workplace empowerment*. Mission command focuses on outcomes, enabling everyone in an organisation to have a clear understanding of the overarching story that the government wants to tell. Therefore, the term 'framework' is apt because it establishes boundaries in which actions, by word or deed, are sure to serve a purpose. The framework must be strategic and understandable by everyone, in order to restrain and enable at the same time.

Strategic objectives. Strategic objectives are the ends of national security strategy. Enduring objectives come from a government consensus on the key tenets of national security, usually laid down in a national security strategy or policy. Strategic objectives tend to be similar across most NATO nations. MCDC's work on hybrid threats identifies three strategic objectives of particular relevance to hybrid threats: [58]

- **Maintaining capacity for independent action**. This is a precondition for any subsequent objectives and ensures that the critical functions of a nation can continue. Maintaining this capacity means identifying and addressing vulnerabilities, then building resilience.
- **Deterring an adversary from taking courses of action**. Effective deterrence persuades an adversary from taking a course of action. The decision by an adversary to escalate or de-escalate is determined by the perception of thresholds established by targeted nations and international organisations.
- **Disrupting or preventing further hostile measures**. This moves beyond deterrence to measures that will disrupt and degrade an adversary's capacity for action.

Narrative. In the context of a StratCom framework, a narrative is a written or spoken account of events and information, arranged in a logical sequence. This is then used as an overarching 'story' to orchestrate activities.[59] The narrative is the centre piece from which means and ways obtain meaning in their application. A nation's narrative, covering what it stands for and believes in, can often be deduced from a national security strategy. Narratives seek to explain the rationale for conducting an activity and the outcome sought. They are expressed as a story arc (a common theme communicated through individual stories, images or actions) that seeks to explain how we arrived at the current situation, defines that situation, and expresses a desired endstate acceptable in the context of the individual narratives of the key stakeholders. By applying classical structures of human storytelling, the emotional appeal is easier to maintain.

Themes. A theme is an overarching concept or intention that provides guidance to activities and communications. Themes are designed for broad application and differ from messages, which are narrowly focused and directed at a specific audience. Activities can be initiated that communicate a specific theme, or communications can be used to frame activities in a preferred, thematic way.

To use an example, communicating the theme *resolve* might mean implementing activities that are specifically created to demonstrate the will of NATO nations to act together. This could be done by deliberately increasing the level of military cooperation with allied nations in a particular geographic region. For activities that are being undertaken for other primary reasons (e.g. exercises or high level meetings), these activities can be presented or framed in a way that projects the *resolve* theme .

Effects. An effect describes the impact (a discernible change) on a target audience, usually articulated as a shift in behaviour or attitude. Effects are the outcomes from our activities and can be desired or undesired (sometimes referred to as 2nd and 3rd order or intended and unintended effects).

StratCom Objectives. StratCom, or communication objectives focus on the overall objectives, achieved through communicative actions, that will support the achievement of strategic objectives. StratCom objectives should be SMART – Specific, Measurable, Achievable, Realistic and Timebound, however at the highest level of guidance such specificity is often a challenge.

Further Planning. The StratCom framework provides direction and guidance to enable the planning with their communicative aspects 'baked-in'. This could include the development of communication campaigns, changes in policy positions or the adjustment of force posture.

Annex A: Framework example, airspace violations.

Annex B: Framework example, GONGO

Annex C: DIMEFIL of potential response options.

ANNEX A

EXAMPLE OF FRAMEWORK: AIRSPACE VIOLATIONS

<table>
<tr><th>Aim</th><th colspan="2">Narrative</th><th>Key Target Audiences</th></tr>
<tr><td>This framework provides direction and guidance to address ongoing incidents of airspace violations.</td><td colspan="2">AVs are a serious violation of sovereignty and pose a significant risk to civilian aircraft. In cooperation with our allies, proportionate measures will be taken to mitigate the impact of AV and to actively counter any aggressive behaviour.

We are an independent nation committed to enable peaceful use of airspace for benign purposes. AVs by foreign military aircraft by contrast are a serious violation of our sovereignty and pose a significant risk to domestic and international air traffic. In cooperation with our allies, proportionate measures will be taken to interdict AV to actively counter any aggressive behaviour in order to restore stable and secure conditions in our skies</td><td>Hostile
• Country X military leadership
• Country X political leadership
• Country X domestic media
• Pro-Country X minority in Country Y

Friendly
• Allied and Partner Nations
• Other nations targeted by AV
• Country Y domestic media

Neutral
• Home population</td></tr>
<tr><th>Background</th><th>Strategic objectives</th><th>StratCom objectives</th><th>Effects</th></tr>
<tr><td rowspan="2">Airspace Violations (AV) occur when an aircraft enters controlled airspace without appropriate clearance. An AV is declared by the Ministry of Defence when:

• Absence of flight plan in Air Traffic Management system, communication with civil Air Traffic Control, active transponder

Transponders transmit aircraft's identifying letters and numbers, call sign, serial number, altitude, air speed, GPS coordinates.

An AV may be a deliberate act intended as:

• Demonstration of military capability and will to act
• Test of military preparedness, patterns of response and international cooperation

Or may not be deliberate, but from:

• Negligence, without any concerted attempt to prevent a violation or rectify the error once made
• Difference in interpretation of disputed boundaries

Risk

• Collision with civilian aircraft
• Loss of public confidence in Country Y ability to defend
• Negative impact on home population attitudes towards leadership
• Risk of AV being normalised as routine military activity</td><td>• Deter hostile acts of territorial violation

• Maintain credibility with allies and within intl institutions</td><td>• Maintain cooperation with allies

• Reduce the incidents of airspace violations

• Generate public confidence in own military</td><td rowspan="2">Desired effects

• Population reassured of military's ability to defend

• Military and political leadership deterred from committing further AV

• Pro-Country X minority in Country Y understand AV are serious violations of Country Y sovereignty

• Military and political leadership engages in dialogue with Country Y

Undesired effects

• Country X leadership interprets reference to military alliance as provocation, leading to continued AV or unintended escalation</td></tr>
<tr><td colspan="2">Themes

Capability and readiness
Country Y Air Force is modern, capable and is integrated with early warning systems. Country Y has also increased military spending, with a focus on enhancing air surveillance capabilities.

Collective defence
Country Y is part of a strong military alliance and can draw on vast military capabilities of other allied and partner nations. Country Y will utilize alliance unity if Country X is not cooperative in ceasing violations.

Safety Country Y prioritizes safety of civilians and civilian aircraft, and therefore does not tolerate military incursions into airspace. It does not tolerate the use of aircraft without transponders turned on and the lack of coordination with Air Traffic Control. Country Y will make AV public, releasing information regarding the timing, location, and frequency of violations.

Dialogue and restraint Country Y has demonstrated restraint in dealing with AV. It is committed to de-escalation and is eager to engage in dialogue with Country X. This dialogue will allow Country X to clarify the violations and to explain their activity. Maintaining dialogue will allow Country Y to retain diplomatic relations with Country X.</td></tr>
</table>

ANNEX B

EXAMPLE OF FRAMEWORK: GOVERNMENT ORGANISED NON-GOVERNMENT ORGANISATION

<table>
<tr><th>Aim</th><th colspan="2">Narrative</th><th>Key Target Audiences</th></tr>
<tr><td>This framework provides direction and guidance to address GONGOs involved with hostile state influence. It provides guidance as a response to hostile influence by GONGOs and to mitigate their future influence.</td><td colspan="2">We tolerate legitimate cultural exchange between nations

This nation rests on a strong identity profiting from the peaceful and tolerant exchange of ideas and culture on the national and international stage. Freedom is always the freedom of the other, thus any form of abusing our liberal discourse for the sake of undermining the very foundations which make this discourse for the benefit of all involves is unacceptable. Any organisation funded by external actors openly or covertly trying to further an agenda to the detriment of our culture of tolerance, and the societal consensus enabling it, will therefore forfeit its right to take part in it.</td><td>Opposing
• GONGO within state
• Political leadership of government linked to GONGO
• Target audience of GONGO activities
• Domestic media under government control
Friendly
• Host institutions
• Other state at risk to hostile influence activities.
• Domestic media
Neutral
• Home population
• International media</td></tr>
<tr><th>Background</th><th>Strategic objectives</th><th>StratCom objectives</th><th>Effects</th></tr>
<tr><td rowspan="2">Definition. A GONGO is a Government-Organised Non-Governmental Organisation which is openly funded, organised or directed by a government in order to extend its influence. GONGOs operate under the guise of non-governmental organisations or civil society groups. They can be established as a tool of public diplomacy, promoting intercultural dialogues and social purposes. However, they can also act as a tool of an adversarial government to further its political interests and achieve domestic or foreign policy objectives in a target state.

Characteristics. GONGOs can manifest as academic groups or institutions, non-profit organisations or advocacy groups, or overseas research institutes. The institutional set-up of GONGOs mirrors NGOs meaning that they can often circumvent certain laws of transparency and accountability.

Risk. GONGOs can be used by states to project influence. The nature of hostile influence can be promoting antidemocratic thoughts and values, undermining the ruling authority, or discouraging the integration process of minority groups with historical or cultural ties to the adversarial government. GONGOs can be used a tool to promote particular narratives whilst dispelling competing narratives. GONGOs have also been associated to censorship and self-censorship issues. GONGOs can influence public opinion to the benefit of the hostile government.</td><td>• Deter hostile influence
• Maintain societal cohesion
• Avoid escalation</td><td>• Deter adversarial government from enabling or direction GONGO to engage in nefarious activity.
• Raise awareness of any hostile activity
• Reduce impact of any ongoing hostile activity</td><td rowspan="2">Desired effects. Hostile political leadership recognises our ability to identify and attribute GONGOs responsible for hostile influence activities

The target audiences of GONGO activities and our home population is aware of adversarial government use of domestic and international media to sow discord and discontent

Hostile actor understands our determination to protect population

Undesired effects. The domestic media under adversarial government control exaggerates our disagreement with GONGO influence activities as a rejection of intercultural exchange

The adversarial government views the countering of hostile GONGOs as a provocation, leading to escalation</td></tr>
<tr><td colspan="2">Themes

Vigilance. We will detect GONGOs that are engaging in hostile influence activities and are able to identify their government that the GONGO is associated to.

Fairness and tolerance. We value freedom of speech and intellectual freedom, and do not seek to stifle academic inquiry. We are aware of the GONGO's attempts to censor sensitive topics, and we will ensure that such censorship is avoided to retain freedom of speech.

Resilience and cooperation. In recognising and engaging with audiences targeted by the GONGO we will enhance societal resilience to current and future hostile GONGO activities.

Through improving resilience, we will diminish our vulnerability to hostile GONGO influence and regarding academic institutions, will retain intellectual freedom.

We will also cooperate with other states exposed to GONGO influence to form an understanding of how target states can diminish vulnerability to GONGO influence.</td></tr>
</table>

ANNEX C

THE DIMEFIL SPECTRUM OF RESPONSE OPTIONS[60]

DIPLOMATIC	INFORMATIONAL	MILITARY	ECONOMIC	FINANCIAL	INTELLIGENCE	LEGAL
Raise issue in international forum, push for joint response with allies	Undertake regional and global info campaigns. Publicise aggression, name and shame	Direct military action to confront with hostile forces	Expulsion from international economic organisations	Attribution of financial wrongdoing (corruption, fraud)	Public communication of the threats by Intelligence services or homeland security	Adopting legislation or regulatory rules to narrow legal ambiguity
Bilateral engagement with allies for joint response	Conduct information campaign in targeted state	Station specific new military capabilities permanently in key locations	Facilitate the expansion of bilateral trade with targeted countries and allies	Enhanced partnerships with the private sector	Identify and engage with susceptible groups vulnerable to infl hostile actors	Specific restrictive measures and sanctions
Use existing instruments available through international institutions	Quick response to capitalise on adversary overreach	Deploy small contingent of mil, law enforcement or civilian personnel on rotational or temporary basis	Push to diversify trade partners	Using international financial institutions to leverage influence	Demonstrate Information exchange with allies	Prosecuting individuals or organisations for illegal behaviour via independent legal process
Remove bilateral relations with hostile states or bar from participation in multilateral arrangements	Improve coordination among cyber resilience and response orgs	Conduct specific, military transit or movement operations to signal intent	Push to pursue alternative energy sources	Targeted sanctions against specific local actors	Expose adversary activities or capabilities using releasable intelligence	Conducting lawfare by exploiting differences in international legal systems to damage a hostile actor's reputation in international fora
Regional diplomatic push to generate a reaction to provocation or aggression	Comms campaigns directed at own society / domestic audience	Conduct ops to relieve or replace local partners to free assets	Suspend development and aid programmes		Build partner intelligence capacity	Enact legal reforms to address disinformation
Improve the timeliness of bilateral and multi lateral responses	Public statements aimed at hostile actors	Announce new exercises, training missions, port visits to targeted countries and others in region	Suspend economic assistance		Deploy intelligence operatives	
Conduct regional outreach to reassure targeted countries	Public statements aimed at allies	Enhance or indicate preparedness to start operations	Deny hostile state participation in key economic institutions			

ENDNOTES

1 Woody, C. (2018, September 19). NATO's top officer says we're living with "a more blurred line between peace and war" — thanks to new Russian tactics. Business Insider Nederland.

2 Heap, B. (2019, September). Hybrid Threats, A Strategic Communications Perspective (ISBN-978-9934-564-33-). NATO Strategic Communications Centre of Excellence.

3 For discussion on this see Cullen, P. J., & Reichborn-Kjennerud, E. (2017). MCDC Countering hybrid warfare project: Understanding hybrid warfare. A Multinational Capability Development Campaign project, London, p.8.

4 It started off as DPE (Psychologic) around the time of the First World War then DME, then DIME. DIMEFIL or MIDFIELD makes an appearance in JDN 1-18

5 NATO, Allied Command Operations (2013). Comprehensive Operations Planning Directive, interim v2.0.

6 Giannopoulos, G., Smith, H., & Theocharidou, M. (2020). The Landscape of Hybrid Threats: A Conceptual Model. Joint Research Centre, Centre of Excellence for Countering Hybrid Threats: Helsinki, Finland.

7 The 'FIL' was added in response to the threat from terrorism, for background see "Putting the "FIL" into "DIME": Growing Joint Understanding of the Instruments of Power"

8 US Department of Defense (2019). Joint Doctrine Note 1-18 Strategy. "Despite how long the DIME has been used for describing the instruments of national power, U.S. policymakers and strategists have long understood that there are many more instruments involved in national security policy development and implementation".

9 Tallis, B., & Šimečka, M. (2016). Collective Defence in the Age of Hybrid Warfare. Institute of International Relations. page 9.

10 Cullen, P. J., & Reichborn-Kjennerud, E. (2017). MCDC Countering hybrid warfare project: Understanding hybrid warfare. Multinational Capability Development Campaign, London, p.11.

11 Ibid.

12 Gates, R. M. (2008, September 29). Secretary of Defense Robert M. Gates' Speech, September 29, 2008 | Armchair General Magazine - We Put YOU in Command!

13 US DoD (2010) Quadrennial Defense Review Report, p.8.

14 NATO (August 2010), Bi-SC Input to a new NATO capstone concept for the military contribution to hybrid threats. SHAPE, Belgium.

15 NATO (March 2021) NATO's Response to Hybrid Threats

16 Russia had used similar tactics in Georgia in 2008 but these were only described as 'hybrid' retrospectively.

17 European Commission (2016), Joint Communication to the European Parliament and the Council, joint framework on countering hybrid threats. p.1.

18 Of note, the framework articulates 'Strategic Communications' in the limited context of a response as a response to disinformation, a significant difference from the NATO concept which inevitably causes friction between practitioners and policy makers.

19 NATO Press. (2019, December 4). Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Heads of State and/or Government. NATO.

20 European Union and Hybrid COE (2020) The Landscape of Hybrid Threats: A Conceptual Model. p.4.

21 Paul Watzlawick, 'One cannot not communicate', referenced in the 'Flows in Media and Communication Blog http://iletisim.ieu.edu.tr/flows/?p=276, retrieved November 2020.

22 Bolt, N., & Haiden, L. (2019). Improving NATO Strategic Communications Terminology. NATO Strategic Communications Centre of Excellence, Riga, Latvia.

23 This is a slight divergence from the NATO definitions in the 2009 and 2016 policies, however while those definitions are practical for NATO StratCom they are too proprietary to be applied generically across the NATO nations in the context of national security strategy.

24 NATO (May 2019), AJP-5: Allied Joint Doctrine for the Planning of Operations – Edition A Version 2 with UK national elements

25 Worley, D. R. (2012). Orchestrating the Instruments of Power. John Hopkins University. P18.

26 One way to think of this is as the physical state of things to be 'data' and their interpretation into meaning as 'information'. An example would be 'Water is falling from the sky' (data), which is interpreted in the mind as 'it's raining' (information). As Paul has pointed out, the fact that the 'information environment' is a conceptual model means that it is difficult to both 'represent and understand'.

27 Pickrell, R. (2019, April 24). The US Navy just sent Russia a powerful message — with 2 aircraft carriers. Insider.

28 Finnish Government Communications Department. (2019, November 8). Joint exercise between Finland and Sweden to focus on preparing for and responding to information influence activities. Valtioneuvosto.

29 Al Arabiya English. (2020, May 20). Hook: Sending US troops to Saudi Arabia sends a powerful message to Iran.
30 Agence France-Presse. (2020, January 8). Indonesia deploys fighter jets, warships to patrol Natuna islands at centre of spat with Beijing. South China Morning Post.
31 Latvian Public Broadcasting. (2020, January 2). Latvia, Estonia, Finland launch joint gas market. LSM.LV.
32 Judson, J. (2019, October 14). Fighting the bureaucracy: For NATO, the Defender 2020 exercise in Europe will test interoperability. Defense News.
33 Kvien, K. (2020, February 6). Remarks by CDA Kristina Kvien at the Announcement of the Head of the National Agency for Prevention of Corruption. U.S. Embassy in Ukraine.
34 Zhen, L. (2019, November 19). US Navy sends littoral combat ships to 'bolster attack strength in South China Sea'. South China Morning Post.
35 Prime Minister's Office, 10 Downing Street. (2018, September 5). PM statement on the Salisbury investigation: 5 September 2018. GOV.UK.
36 Laity, M. (March 2018). NATO Strategic Communications, The story so far. NATO Joint Warfare Centre, Three Swords Magazine. p 71.
37 UK Ministry of Defence (2015), AJP 3.14 Allied Joint Doctrine for Force Protection, Edition A, Version 1. p.1-1.
38 Monaghan, S., Cullen, P., & Wegge, N. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. Multinational Capability Development Campaign.
39 UK Ministry of Defence (2016), Joint Doctrine Publication 04, Understanding and Decision-making. 2nd edition.
40 Ibid.
41 Gruppe Informationsoperationen, Zentrum für Operative Information der Bundeswehr, (October 2010) Multinational Experiment 6, Enhanced Systemic Understanding of the Information Environment in Complex Crisis Management Analytical Concept. Version 1.0.
42 UK Ministry of Defence (2011), Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations. 3rd Edition. p.29.
43 Antoniades, A., Miskimmon, A., & O'Loughlin, B. (2010). Great power politics and strategic narratives. The Centre for Global Political Economy, Brighton: University of Sussex. Page 1.
44 Cullen, P. J., & Reichborn-Kjennerud, E. (2017). MCDC Countering hybrid warfare project: Understanding hybrid warfare. A Multinational Capability Development Campaign project, London, p.11.
45 Ibid, p.11.
46 Gruppe Informationsoperationen, Zentrum für Operative Information der Bundeswehr, (October 2010) Multinational Experiment 6, Enhanced Systemic Understanding of the Information Environment in Complex Crisis Management Analytical Concept. Version 1.0. p 69
47 'Audience insight' is a useful term as it reflects the challenge that audiences may never be fully 'understood'.
48 Monaghan, S., Cullen, P., & Wegge, N. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. Multinational Capability Development Campaign MCDC.
49 The Lightning Press, The Instruments of National Power, accessed 29 October 2018
50 Ibid.
51 Ibid.
52 U.S. Headquarters Department of the Army (Sept 2008), Army Special Operations Forces Unconventional Warfare. p 2-6.
53 Ibid. p 2-7.
54 Ibid.
55 Ibid, p 2-8.
56 Other formats include SCAEF, favoured by the UK, or an Information strategy.
57 Often referred to as 'Information Activities'.
58 Monaghan, S., Cullen, P., & Wegge, N. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. Multinational Capability Development Campaign.
59 Bolt, N., & Haiden, L. (2019). Improving NATO Strategic Communications terminology. NATO StratCom COE, Riga, Latvia. p56.
60 This draws from RAND's work on responses to below threshold threats. See Morris, Lyle & Mazarr, Michael & Hornung, Jeffrey & Pezard, Stephanie & Binnendijk, Anika & Kepe, Marta. (2019). Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War. 10.7249/RR2942.

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