COI HYBRID INFLUENCE

Hybrid CoE Paper 3

MAY 2020

Tackling the bureaucratic vulnerability: an A to Z for practitioners

Hybrid CoE

Hybrid CoE Papers include inspiration papers, conception papers, and the finalized outcomes of our seminars, workshops, exercises or other activities. They include understandings of currently unfolding events, and analysis or personal views relating to the realm of hybrid threats.

The COI on Hybrid Influencing looks at how state and non-state actors conduct influence activities targeted at member states and institu-tions, as part of a hybrid campaign. The COI looks at how hostile state actors use their influence tools in manners that attempt to sow instability or curtail the sovereignty of other nations and independence of institutions. The focus is on both the behaviours, activities, and tools that a hostile actor use, rather than focusing exclusively on one actor at the expense of of others. The goal of the community is to equip its practitioners with the tools they need to respond to and deter hybrid threats. of others. The goal of the community is to equip its practitioners with the tools they need to respond to and deter hybrid threats.

The COI on Hybrid Influencing has a sub-COI called Non-state actors and looks how different proxies and other non-state actors conduct influence, on behalf of hostile state actors. The sub COI is led by Sweden.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

IISBN 978-952-7282-40-3
ISSN 2670-2053

May 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Tackling the bureaucratic vulnerability: an A to Z[1] for practitioners

Introduction

There is one vulnerability that all states and institutions share when it comes to tackling hybrid threats – their own bureaucratic vulnerability. Symptoms of this vulnerability include the inability to work effectively across government departments and units, poor information flow, competition for resources and influence, and incoherent public messaging. As hybrid threats comprise the use of multiple tools, vectors and activities in coordination (with malign intent), they challenge the coherence and cohesion of bureaucracies, exploiting blind spots and targeting vulnerabilities. The origins of such bureaucratic vulnerability lie in the range of ministries in which different states choose to place the hybrid threat file. Some put it in the Ministry of Defence, linking it to hard security. Others place it in the Ministry of the Interior, emphasizing resilience and the civil dimension. Still others put it in the Chancery or Prime Minister's Office, stressing the cross-government nature of the response.

Luckily, the bureaucratic vulnerability is also one that can be tackled. Once addressed, it is a critical enabler in making modern deterrence work (a key tool for countering hybrid threats), facilitating effective strategies to counter electoral interference and improve/act on situational awareness, for example. Based on cooperation with Hybrid CoE participating states, the EU and NATO over the last three years (including on elections, deterrence and situational awareness), the Community of Interest on Hybrid Influencing proposes the following A to Z of tools, tips and principles for overcoming bureaucratic vulnerability. This is not the final word, but a collection of what has been found to work and what has not by collaborating directly with practitioners in the field. Improving cross-government cooperation will also have second order effects for other non-security-related policy areas, including crisis response.

A to Z

A **gility.** To effectively counter a hybrid action, states need to move quickly and energize multiple parts of the government at once. Having legislative instruments available to facilitate swift action in a time of crisis is important. Government responses to hybrid threats require swift decision-making and multiple redundancies. One of the most effective ways to build agility is through repeated exercises [and scenario mapping] that look at all phases of a hybrid attack, helping to:

- build staff capability;
- create communities and teams across government;
- test the flow of information;
- allocate resources and responsibilities;
- develop connectivity between government departments and divisions;
- build resilience in response mechanisms.

1 We would like to express our thanks to colleagues who have commented on this paper in draft form, including Harri Ohra-aho and Dr James Pamment, as well as our appreciation of the insights and thoughts provided by the practitioners we have trained, brainstormed with and worked with over the last three years.

Bureaucratic politics.[2] Competition for resources or political influence between government departments is inevitable, but it is corrosive and fuels the bureaucratic vulnerability. It is critical to gather the broadest array of policymakers around the table from a range of (both security and non-security) ministries, so that multiple interests are represented in policy development. The widest range of departments should feel that they have a stake in the development of policy on hybrid threats and in crisis response.[3]

Challenge (internal and external red teams). Some bureaucratic systems favour consensus-seeking behaviour in their policy processes. This is an important part of bringing multiple voices together to ensure support for a policy position. But challenge (both internal and external) should be baked into policymaking on hybrid action. This can be realized through the creation of a trusted and security-cleared "red team" of experts on a specific actor that uses hybrid threats. This red team can test the effectiveness and impact of a policy decision designed to influence the behaviour of those who use hybrid threats. This can be within the context of an exercise or outside of it as part of a policymaking sign-off/clearance process.

Diversity. Many hands make light work, many diverse voices make better policy. Adversaries use hybrid threats to exploit gaps between government departments as well as societal divisions, and look to prise these apart to sow discord and mistrust within governments and societies. If policy benefits from a range of diverse voices when it is formulated, it limits the ability of an actor that uses hybrid threats to exploit these differences, and it also challenges internal "group think". Security policy departments should consider recruiting from a diverse range of ethnic, gender and socio-economic backgrounds to improve and broaden the thinking that contributes to policy development.

Empowerment. There are multiple models for organizing a "whole-of-government approach". A **single responsible individual** who is suitably empowered to convene relevant cross-government colleagues working on hybrid threats is an effective way of making a whole-of-government approach work. This senior responsible individual should own the delivery and be accountable for the government's policy on countering hybrid threats. They should be able to compel personnel across government to analyse, develop and challenge policy on hybrid. They do not require a large secretariat (indeed this could create another competing division), but need to have significant influence and be senior enough to engage at a senior level across government and the private sector, and with political decision-makers. Non-security ministries should also appoint a working-level hybrid lead (who is familiar with security issues) to dock into the wider cross-government effort.

Fusion. Information fusion across government is a critical enabler. The fusion of a variety of sources, both open and closed, supports more effective information to inform decision- making a nd situational awareness. Sometimes the fusion of intelligence material is not possible as it puts sources at risk. Where they can, intelligence agencies should invest resources in sanitising and declassifying reports so they can be shared more widely.

Government – Where you sit doesn't matter. The **senior responsible individual** can sit in any ministry. It is his/her character, expertise, personality and passion that will be determinative of the impact and effectiveness of the government policy, not his/her home department (don't necessarily give it to the person or department who wants it the most). A senior responsible individual must, however, be able to corral participation and compliance on relevant issues across all departments and ministries.

2 Graham T. Allison and Morton H. Halperin, *World Politics* Vol. 24, Supplement: Theory and Policy in International Relations (Spring, 1972), pp. 40–79.
3 A non-exhaustive list, but consider including the following departments: education, employment, trade, culture/media, health, infrastructure, and energy.

Human Resources (HR) policy. Existing government HR policies tend to (rightly) reward achievement in a practitioner's area of responsibility, or for contributing to that department's strategic objectives. Recognition of a contribution to another government department's objectives, or to a wider cross-government effort is less common. Possible ways to address this include:

- seeking feedback on a practitioner's work from outside of their ministry.
- recognition of a practitioner's work in support of other ministries within annual appraisals/ reports.

Another dimension of HR policy that may need to be boosted is the recruitment of appropriately security-cleared personnel across government departments. More funding may need to be invested in security vetting to be able to bring in expertise from outside of government.

IT systems. Competing government IT systems repeatedly surface as a challenge for practitioners. At a baseline, different government departments' IT systems need to be able to talk to each other and share relevant classified material. In practitioners' experience, physical or appropriately protected virtual meetings still provide the best forum for information-sharing (see **V**, **X**).

Joint discussion of the threat picture. Closely linked to **F**, a joint discussion of the threat picture, drawing on information from cross-government intelligence agencies and open source material is key as a baseline for evaluating response options. Competing threat perceptions can make evaluating resilience and response options more challenging. A joint discussion of the threat picture recognizes different assessments (and these are of course an important part of the challenge process). This discussion should take place at as low a classification as possible to allow for inclusivity to raise awareness of decision-makers in non-security government ministries. This process is most effective when it is part of the drafting of cross-sectoral strategies, white books or other documents that eventually capture this shared threat picture.

Knowledge. Expertise should be retained and shared across government departments. Knowledge and a shared understanding of a state's own vulnerabilities and weaknesses are particularly important when developing a strategy to counter hybrid threats, as is knowledge of those who use hybrid means when crafting deterrence strategies that focus on holding their values, interests, and vulnerabilities at risk. Having appropriate knowledge also supports the intelligence-gathering processes, helping practitioners to send the right RFIs (requests for information) to the intelligence agencies and to ask the right questions. This could involve:

- the regular inclusion of analysts in policy meetings.
- bringing in outside expertise to challenge thinking and check assumptions (see **C**).

Language. Another factor that can make cross-government cooperation more challenging is the absence of shared language to talk about hybrid threats within government. It is not uncommon to find different government departments using different terms to talk about the same hybrid activity. While dwelling too long on definitional issues can divert time and resources, a brief set of meetings with a short deadline aimed at developing a series of inclusive terms and definitions to describe key terms could help. Alternatively, a quick set of decisions that establish which terms will be used across government can be beneficial.

Multilateral. Working multilaterally with international partners can support cross-government working through:

- creating shared assessments;
- multiplying the effect of responses;
- gaining access to another state's expertise;
- access to allied channels with regard to adversaries;
- broadened credibility offered by solidarity/ joint efforts;
- access to unique multilateral measures (sanctions etc);
- de-confliction with allied bureaucracies and burden-sharing.

To gain the maximum benefit from working multilaterally, governments should consider how to coordinate their engagement with partners, so that their messaging and any asks are coherent. A cross-government strategy (and accompanying meeting) that brings together all initiatives across government relating to a particular partner can support this process. It can be useful to appoint a single empowered individual who has oversight when it comes to delivering the strategy.

"Normal"/Not everything is a hybrid threat. There are two challenges here. First, not everything is a hybrid threat. Making a distinction between what is unusual and possibly malign and intentional and what is simply unusual can be difficult, and having a shared understanding of this across government can be even more challenging. To determine what "normal" looks like, it can be helpful to:

- Identify sectors that require special protection.
- Baseline what normal operations look like.
- Bring together sectoral monitoring into a government-wide picture, as well as bringing sectoral specialists together in an X-government meeting (see **X**).
- Brief private sector actors (particularly in critical infrastructure) on emerging trends and exchange and share analysis.
- Acknowledge that creating a "normal" baseline takes time (2–5 years).

Sectoral experts will be best placed to assess what "normal" looks like. Cross-government situational centres can provide a combined picture, but they need:

- appropriate data feeds from government, private and public sectors;
- to broadly distribute an example pack of the kind of activity that can be termed hybrid;
- to be sufficiently empowered bureaucratically to feed into joint intelligence assessments.

Open source. Intelligence improves situational awareness. It supports understanding and provides a solid evidence base that can be readily communicated to the population and shared horizontally with allies. It can also be used in court (unlike classified material) and can support attribution. It is therefore distinct from intelligence material in character. The trend of creating open source intelligence cells or units across government has been welcome and has improved many nations' capabilities to counter hybrid threats. Where possible, they should share their information across government, rather than creating multiple open source units within individual government ministries. Special attention needs to be paid to how this data is communicated to senior decision-makers. "Big Data" can sometimes be hard to digest. Open source analysts may need support and training to be able to communicate their product effectively.

Private sector partnership. Governments no longer have a monopoly on the information, tools and responses required to develop situational awareness, to counter electoral interference or to implement a deterrence posture. The private sector has significant information relevant to government decision-making and also has the power to attribute and deter hybrid activity (as well as a commercial interest in doing so).

Many government sectoral practitioners have effective existing relationships with the private sector. But these relationships sometimes exist in silos, separate from one another. Links between government analysts and threat disruption teams are particularly important. Seeking out opportunities to meet with threat disruption teams from other states can be helpful, as social media platforms often do not have the capacity to engage with each state individually. What is sometimes missing is the relationship at a strategic level between senior-level government officials and senior corporate leaders, so states can have a clear picture of the overall government relationship with a particular private sector actor.

Don't stay quiet… Hybrid threats can affect different sectors and can be observed by different stakeholders. Practitioners and specialists often think that unusual activity is nothing to report because it may appear minor or trivial. This could lead to a situation where an ongoing hybrid

campaign could be overlooked (including the cumulative effect of various interferences across different domains). Practitioners have found it useful to adopt an approach whereby anything that looks unusual should be reported, rather than staying quiet about it.

Resources and relationships. Effective cross-government working does not always require more resources but may be about organizing existing human and financial resources more effectively. In fact, some smaller nations are better able to share information precisely because there are fewer people to share it with. Developing a cross-government community that know each other well and have strong relationships can overcome information-sharing challenges. This could take the form of a cross-government taskforce, a community of interest or a cross-government working group. Trust is a critical feature in these relationships if they are to work effectively, particularly in a crisis. There may be historical or cultural reasons for mistrust between ministries. One way of overcoming this can be strong leadership and modelling collaborative behaviour at the very highest levels between ministries and their political leadership.

Sharing. Different departments have different sharing cultures. Collectively establishing the culture and norms that will govern the hybrid policy-making community can be a useful starting point. Some material will remain on a need-to-know basis, but a two-pronged approach could include:

- creating a larger, wider pool of appropriately cleared individuals who can access classified material (which will also pay dividends in times of crisis, when resilience within networks is important);
- incentivizing the sharing of information, by singling out examples of appropriate information-sharing for recognition.

Time (and institutional memory). Bureaucratic institutional memory is a critical enabler in overcoming bureaucratic vulnerability, serving to mitigate the effects of constant staff turnover. Good institutional memory can also prevent conflicts between departments by setting out how issues were handled in the past (which government department was responsible), and saves time by reminding practitioners about previous conceptual and policy debates. Improved institutional memory can be achieved through:

- effective archiving;
- institutional memory added to job descriptions of government analysts;
- senior decision-makers adding "Have we seen this before?" to X-government ops/intel briefings (see **X**), ascertaining who the lead was, and whether they are available to advise.

Unified messaging across government. One symptom of bureaucratic vulnerability can be multiple different messages emanating from different parts of government. Clear, planned coherent communication can reinforce effective cross-government cooperation. Strategic communicators and press officers (depending on the type of issue) consequently need to be integrated into policymaking from the start (they can and should, for example, participate in the X-government meeting – see **X**). Moreover, communicators need to be in regular contact with one another, to which end creating a communication cadre or profession across government can be helpful. This will enable government departments to complement each other's messages and reach a greater variety of audiences, rather than competing.

Virtual communities. One of the biggest challenges states face when tackling hybrid threats is that practitioners who work on these issues are often unacquainted with each other. Creating communities where colleagues know each other can overcome the challenges of information-sharing. These communities could be created through joint participation in a meeting (see **X**) or by attending training. Hints for keeping the community alive include:

- having a regular meeting time. This makes a "habit" out of connection.
- feeding the community material in between

meetings, whether it concerns sharing useful articles or resources.
- appointing/nominating somebody to curate the community and keep it alive.
- looking at establishing the community on a group messaging service alongside email, allowing for quicker reactions.

Why, what, when? Gaining an X-government understanding of the following questions (drawing on information from across government) can support the development of a strategy for countering hybrid threats:
What forms do hybrid threats take?
What are the strategic goals of those who use hybrid threats?
Why are they resorting to hybrid threats?
Where and how should government respond?

Considering why an actor is using hybrid threats supports the development of effective response options, including deterrence. By asking what their strategic goals are, it is possible to develop an actor-specific strategy that holds their vulnerabilities, values and interests at risk. By understanding these two factors, it is possible to prepare for a hybrid attack, and also to consider the timing of one's response.

X-government operations and policy meetings. An effective way of exchanging information and improving situational awareness is hosting weekly X-government operations and policy meetings on hybrid threats. Top tips for making these meetings useful include:

- Getting the invitation list right. Think beyond traditional security and intelligence agencies. Include departments covering trade and investment, critical national infrastructure, transport and education.
- Holding them at the lowest classification possible, initially to ensure the broadest participation and to allow everyone to contribute. If necessary, have a higher classification follow-on meeting (but these two meetings should avoid creating two separate communities). The low-classification meeting should be where the bulk of the business is handled.
- Having a document to discuss. This could be a matrix/dashboard of indicators across sectors, which can frame discussions.
- Using them as an opportunity to debrief on political decision-makers' views and to prepare for ministerial meetings.
- Recording actions clearly and following up.

Yearly review. Conducting a light-touch annual review of cross-government cooperation can be useful for evaluating new structures and identifying lessons.

Your priorities. A centralized process for determining priorities across government in relation to hybrid can be beneficial for focusing on policy objectives. These can be determined by asking:

- What are our vulnerabilities?
- What are the critical national interests that need protecting?
- How can this be achieved within our means and resources?

Although each bureaucracy understandably has its own challenges, competing departmental priorities on hybrid can worsen the bureaucratic vulnerability (something that those who use hybrid threats would like to see happen). An inclusive policymaking process to develop cross-government priorities on hybrid can be beneficial and ensure that resources are used most effectively and conflicts avoided.

"Zoom out". Hybrid threats occur in a broader security context. One area that can cause friction within governments (and that heightens the bureaucratic vulnerability) is the assumption that work on hybrid threats will displace traditional security policymaking (and the investment within it). It should not. Traditional security policy – including investment in deterrence and conventional operations – remains important and plays a crucial role in countering hybrid threats.

Reassurance is key as new decision-making mechanisms are created and senior responsible individuals take up their duties. They should work alongside existing government structures. Early meetings with existing security stakeholders are an important way of building trust; looking at areas for collaboration where quick wins can demonstrate the impact of this new work area is key. Having a senior responsible individual acting as a convener for cross- government discussions can be a useful way of building trust.


Hybrid CoE