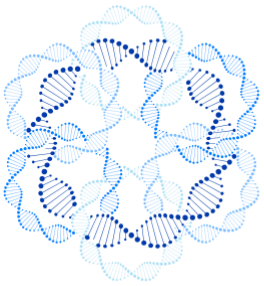


THE AZURE FORUM
FOR CONTEMPORARY SECURITY STRATEGY

Statement to the Oireachtas Joint Committee on Foreign Affairs and Defence

"Disinformation and hybrid threats from the context of geopolitical shifts"

Caitríona Heinl, Executive Director, Azure Forum for Contemporary Security Strategy

Tuesday 16 May 2023

This statement describes the nature of hybrid threats within the context of geopolitical shifts and strategic threat assessments. It especially focuses on the nexus with 'disinformation' and cyber; the threat landscape; notable evolving trends; and examples of good practice solutions. It aims to emphasise the constantly changing nature of hybrid threats and their import to nation states, including Ireland.

Definition and common understanding from a geopolitical perspective – a combination of 'new wine' and 'old wine in new bottles'

Establishing a baseline common understanding of the hybrid threat is essential to developing appropriate national, regional and international responses.

'What'

While there is no agreed definition, hybrid threats are understood to comprise a **combination of different types of tools**, some expected and known, some unexpected and clandestine, applied to achieve an undeclared strategic objective.[1]

'Why'

Broadly speaking, hybrid threat actors **aim to undermine or harm** democratically established governments, countries or alliances.[2] The European Commission's Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) explain that hybrid threat actors aim to:[3]

- Undermine and harm the integrity and functioning of democracies by targeting vulnerabilities of different domains, creating new vulnerabilities through interference activity, exploiting potential weaknesses, creating ambiguity and undermining the trust of citizens in democratic institutions;
- Manipulate established decision-making processes by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear factors in target societies; and
- Maximise impact by creating cascading effects, notably by tailoring attacks, combining elements from specific domains to overload even the best prepared systems, with unpredictable, negative consequences.

In short, overarching objectives include "**undermining public trust in democratic institutions, deepening unhealthy polarisation both nationally and internationally, 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**".[4]

[1] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., *Hybrid threats: a comprehensive resilience ecosystem – Executive summary*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019.

[2] Ibid.

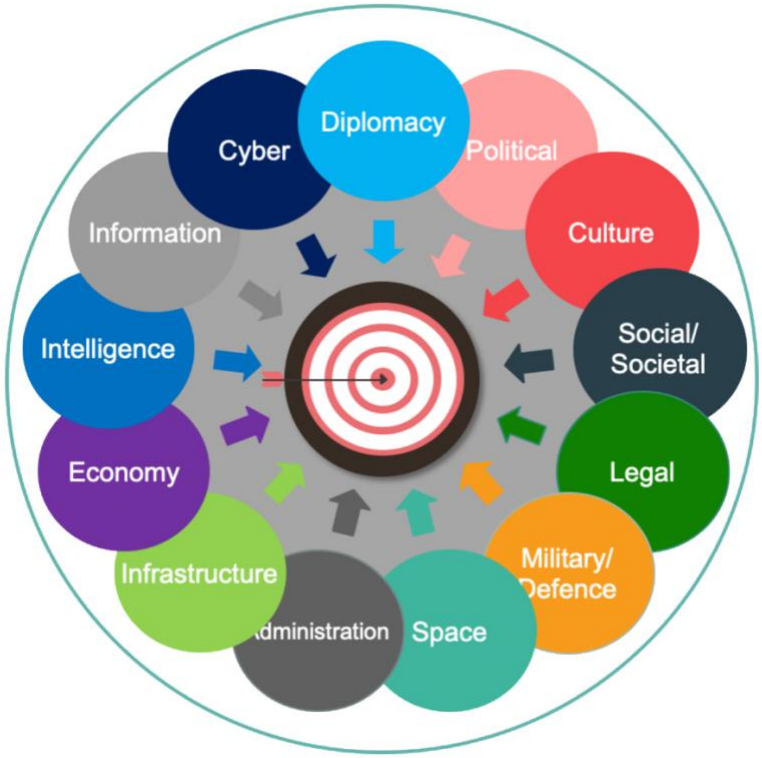
[3] Ibid.

[4] https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

'Who' and 'How'

Both **state and non-state actors** undertake hybrid activity. Non-state actors' activity can include non-state hybrid threats independent of state influence as well as the undertaking of state hybrid threat activities through non-state actor clients (such as a proxy).[5]

Hybrid attacks and campaigns can be understood as **coordinated actions across different domains** – for example, cyber attacks that include information manipulation with a view to influencing electoral outcomes. Different types of tools and organised actions such as disinformation, economic pressure, abuse of migrants, cyber attacks and other covert actions are understood as being combined.[6] The image below provides a visual depiction of the wide **breadth of domains and tools relevant to nefarious hybrid activity**.[7] The table in Annex 1 provides further detail on the extensive nature of tools for hybrid activity. Notably, state and non-state foreign actors are observed to be **constantly refining their tactics, techniques and procedures**.[8]



Understanding the cyber and disinformation/FIMI nexus in the context of hybrid threats

[5] For detailed information, see Hybrid CoE Research Report 6, 'Hybrid threats from non-state actors: A taxonomy', Janne Jokinen, Magnus Normark, Michael Fredholm, June 2022.

[6] https://joint-research-centre.ec.europa.eu/jrc-news/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en

[7] https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

[8] Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence, Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council, March 2023.

The EU's 2020 Cybersecurity Strategy explains how **hybrid threats can combine disinformation campaigns with cyber attacks** on infrastructure, economic processes and democratic institutions, with the potential for causing physical damage, obtaining unlawful access to personal data, stealing industrial or state secrets, sowing mistrust and weakening social cohesion - these activities **undermine international security and stability and the benefits that cyberspace brings for economic, social and political development**.[9] As part of wider hybrid operations in recent times, cyber-enabled influence know-how that seeks political, diplomatic, economic and military advantage is becoming more prolific. The current national cybersecurity strategy for Ireland includes a section on hybrid threats, explaining that **many hybrid threats have had a cyber component**, finding that the most common of which has been the use of cyber tools to steal information for subsequent use in disinformation campaigns (so-called 'hack and leak').[10] It then explains that as an open liberal democracy, Ireland is vulnerable to campaigns of this type in much the same way as other EU Member States.

Similarly, the first 'Annual Progress Report on the Implementation of the EU Strategic Compass for Security and Defence', released in March 2023, specifies how 'Foreign Information Manipulation and Interference' **(FIMI) is increasingly used as part of broader hybrid campaigns**.[11]

While so-called 'disinformation' is not a new issue, it has become well recognised that what is new is how it is produced, distributed and the ways in which individuals, entities or states can be targeted. Although there is a tendency to perceive of this problem as a societal issue only in terms of how information is used, there is **now an accepted need to understand that it is far more than a societal issue**. In other words, there is a **need to distinguish what is disinformation and what is security-related**.

It is also a **security challenge comprising the deliberate activity of actors that use the information environment and manipulation of the information environment as a strategic tool**.

It is coordinated intentional activity used as a security instrument where major financial and other resources are being used (thus warranting the use of the term 'foreign information manipulation and interference'). This activity is not just about narratives. It comprises different forms such as (1) Manipulation of content that is not always a falsehood (such as reinforcement of existing views or putting things out of context); (2) Manipulation of identities comprising working with false identities (such as false accounts); and (3) Manipulation of reach, meaning that techniques are used to amplify messages (such as troll farms; competing narratives; targeting vulnerable groups such as minorities; targeting conspiracy groups; 'throwing mud to the wall' meaning that all sorts of narratives are used in the hope that something will stick.[12]

[9] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 'The EU's Cybersecurity Strategy for the Digital Decade', 16 December 2020.
[10] Government of Ireland, 'National Cyber Security Strategy 2019-2024'.
[11] Annual Progress Report, Strategic Compass, March 2023.
[12] Author observations, EU-ASEAN dialogue on enhancing security cooperation, held under the Chatham House rule, Brussels, June 2022.

In the Irish context, even though the findings of the July 2022 Report of the Future of Media Commission included, for example, a recommendation for a national [counter] disinformation strategy, it seems that the conception of 'disinformation' through such processes have not been overly focused on the geostrategic/security aspects with a FIMI/hybrid threat lens.

International threat landscape and notable evolving trends – 'weaponisation of everything'

Regular, strategic threat assessments are necessary to develop better national security strategy and, by extension, national responses to hybrid threats in the context of a constantly changing strategic/geopolitical environment.

By way of example, at regional EU level, the first ever EU Threat Analysis was conducted in 2020 in order to properly prepare the EU Strategic Compass. The Compass provides the EU's pathway on security and defence for the next five to ten years in relation to the strategic environment. An update of the EU threat analysis was conducted in December 2022.

Even though the EU threat analysis remains classified, the Strategic Compass does elucidate the following **hybrid threat related trends in the geostrategic landscape**:

- Hybrid threats are **growing both in frequency and impact**.
- In Ukraine, as elsewhere, the tools of power are not only soldiers, tanks and planes but also financial sanctions or import and export bans, as well as energy flows, and disinformation and foreign interference operations. There has also been examples of the instrumentalisation of migrants, the privatisation of armies and the politicisation of the control of sensitive technologies.
- State and non-state actors are using hybrid strategies, cyber attacks, disinformation campaigns, direct interference in elections and political processes, economic coercion and the instrumentalisation of irregular migration flows.
- The EU is facing increasing attempts of economic and energy coercion.
- The increasing misuse of law (so-called lawfare) to achieve political, economic and military objectives is a growing concern.
- Competitors are not shying away from using Emerging and Disruptive Technologies (EDTs) to increase the effectiveness of their hybrid campaigns.
- Some competitors have seized on the uncertainties created by the Covid-19 pandemic to spread harmful and false narratives.
- In relation to the **armed aggression against Ukraine**, the Compass finds that Russia is showing readiness to use the highest level of military forces, combined with hybrid tactics, cyber attacks and FIMI, economic and energy coercion. The nation is also said

to use crises in an opportunistic way, including by using disinformation and mercenaries as well as actively interfering through hybrid tactics, compromising the stability of countries and their democratic processes, which is viewed as having direct implications for European security.

- Other nation states are described within the Compass document as displaying hybrid tactics too.

The more recent March 2023 'Annual Report on the Implementation of the Strategic Compass' reiterates that state and non-state actors are increasingly using hybrid tactics against the EU, its Member States and partners, a trend exacerbated by Russia's invasion of Ukraine. It notes especially the **instrumentalisation** of food, irregular migration, energy and lawfare, amongst other items such as coercion targeting economic and energy security. Hybrid threats continue to be perceived as becoming more sophisticated.[13]

In addition, several notable **evolving and emerging trends** are highlighted below:

- At the end of 2022, the EU Agency for Cybersecurity (ENISA) identification of the top ten emerging cybersecurity threats to likely emerge by 2030 included advanced disinformation campaigns and the rise of advanced hybrid threats.[14]

- Hybrid threats are expected to grow in frequency, impact and scale in future.[15]

- The 2023 U.S. annual threat assessment identifies that efforts by Russia, China, and other countries to promote authoritarianism and spread disinformation is helping **fuel a larger competition between democratic and authoritarian forms of government**. **This competition exploits global information flows to gain influence and impacts nearly all countries**, **contributing to democratic backsliding**, **threats of political instability, and violent societal conflict through misinformation and disinformation**.[16]

- In addition to concerns about nefarious information activity inside our nation states, there are **indicators about the expansion of malign influence globally**, including in Africa and other regions.

- [17]**Some democratic states have been observed as engaging in digital repressions**, **contributing to democratic backsliding** and erosion. Many foreign governments have become adept at the tools of digital repression, employing censorship,

[13] https://joint-research-centre.ec.europa.eu/jrc-news/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en
[14] https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030
[15] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019, April 2023.
[16] For example, see the 'Annual Threat Assessment of the U.S. Intelligence Community', Office of the Director of National Intelligence, 06 February 2023.
[17] Ibid.

misinformation and disinformation, mass surveillance, and invasive spyware to suppress freedom. Digital repression is **occurring against the backdrop of broader digital influence operations that many autocrats are conducting globally to try to shape how foreign publics view their regimes, create social and political upheaval in some democracies, shift policies, and sway voters' perspectives and preferences**.

- There are **indicators of increasing use of EDTs for future geostrategic information purposes**:
    - Analysts find that some states are recognising that artificial intelligence **(AI) as a powerful information tool could target societies and political establishments by impacting the content, speed and volume of data and information delivery and perception**.[18]

    - U.S. threat assessments from early 2023[19] find that **large-scale simulation and the accumulation and analysis of massive amounts of data** are revolutionising many areas of science and engineering research with the potential to influence the future battlefield and shape political discourse through disinformation operations. States are observed as acquiring and analysing personally identifiable citizen information, commercial and government data to make their espionage, influence, kinetic and cyber attack operations more effective; advance their exploitation of the economy; and give them strategic advantage.

Examine and adapt good practice approaches to enhance resilience and counter hybrid influencing

National and EU conceptual approaches to hybrid threats and resilience continue to develop and mature.

Measures are needed to assure citizens and business that better mechanisms are being put in place to safeguard our values, to remain economically competitive, to protect our strategic assets, and to ensure that our nations continue to be a safe and secure place free from future external interference. Such measures would clearly need to extend beyond a focus on safeguarding the electoral system or strengthening the regulation of online media.

Some examples of good practice measures are outlined below (but are far from exhaustive). By way of case study, Annex 2 provides a short 'primer' on Finland's approach to hybrid influencing with a view to exhibiting a practical overview of the complexity and breadth of measures that are being put in place by another EU nation state.[20]

[18] Samuel Bendett, CNA, 'Russian military debates AI development and use', Azure Forum Strategic Insight, 04 May 2023.
[19] Annual Threat Assessment of the U.S. Intelligence Community, 2023.
[20] 'Maturing national responses to hybrid influencing and cyber threats: A primer on Finland's approach', Azure Forum Strategic Insight, Jarmo Sareva, Ambassador for Cyber Affairs and Liisa Talonpoika, Ambassador for Hybrid Affairs at the Ministry for Foreign Affairs of Finland, 02 March 2022.

1.Establishing a baseline common understanding of the hybrid threat is essential to developing out appropriate national responses.

2.Regular, strategic threat assessments are necessary to develop better responses to hybrid threats.

3.A coordinated, cross-governmental approach is important given the combined and coordinated nature of hybrid tactics
An **overarching national framework would bring different relevant instruments together to detect, prepare for and respond in a coordinated manner to the breadth of combined hybrid threats**. Including, for example, cyber mechanisms, the establishment of mechanisms to deal with FIMI, and economic resilience tools, among others (e.g. strategic investment screening mechanisms; export control regimes; 'de-risking' and reduction of economic dependencies' approaches).

4.Increase situational awareness
There is widespread acknowledgement that there is **still a large gap in understanding** about what is happening.

Deeper clarity is needed about who are the actors; their tools, tactics and techniques; the nature of the threat level in order to judge if actions are required or not; distilling how to distinguish what is disinformation and what is security-related, including learning from methodologies created by partners. Enhanced intelligence capacities to detect, identify and analyse these threats and their source would likely also be needed.

5.Build out societal resilience – Develop 'whole of society' solutions
It is acknowledged that this can be very difficult to achieve. It is important to examine and implement solutions that clarify what is the role of the government, private sector and civil society in protecting against this threat. For example, "raising resilience to FIMI is by definition a whole-of-society effort".[21]

- **Governmental strategic communication mechanisms are necessary** as a key capability that provides a source of **verifiable governmental content (outside times of crisis and during peacetime)**. Strategic communications' efforts, their value, structure and approach, including how this would be tailored to the specific Irish context for this specific geostrategic problem set should be examined.
    - Note the new development in the preceding period before the invasion of Ukraine whereby intelligence was declassified and communicated as a counter-disinformation method. This is **one of the latest evolutions** whereby advanced state players' intelligence agencies are **communicating more transparently on intelligence and national security matters** (while also protecting sources and methods) with a view to **bringing about consequences for nefarious actors**.

[21] https://www.eeas.europa.eu/eeas/beyond-disinformation-%E2%80%93-eu-responses-threat-foreign-information-manipulation_en

- As has been the case across several states with maturing approaches to cybersecurity in recent years, it has become good practice to **communicate transparently that government does not have all the solutions and it must work together with the whole of society**. No government or cybersecurity practitioner alone holds all the answers.
- Annex 3 provides a draft example of some relevant lessons from experts involved in recent crisis communications in the Irish context.

- There is a need for **support to non-governmental, independent research enterprises**[22] and **engagement with the media to inform independent content and provide additional sources for trust reasons**. This would **foster a fact-based information environment** and counter the impact of state-controlled foreign outlets. This could include working with media and awareness raising campaigns; media literacy; supporting researchers; fact checking organisations; and developing capability to do this which will require working with many partners and governments to develop these structures and approaches. This could assist the public's ability to **access information from many trusted sources**.

6. International cooperation: Continue to draw on, learn from and engage with EU responses and like-minded partners

Examples of **good practice EU initiatives** include the following:

- The EU Hybrid toolbox aims to bring different instruments together to detect, prepare for and respond in a coordinated manner to a broad range of hybrid threats. It acts as an overall framework to bring together relevant mechanisms such as the cyber diplomacy toolbox and the FIMI toolbox. In 2022, the Council of the EU agreed a Framework for a coordinated EU response to hybrid campaigns and work has been undertaken on the development of implementing guidelines, which with the Framework, will become key components of the Hybrid Toolbox.[23]

- The Hybrid CoE can assist with **ongoing capability development** through, for instance, the provision of training or exercises. Ireland became a member in January 2023, with access to strengthen its capacity building to prevent and counter hybrid threats.

- **New methodologies** are regularly released by the Hybrid CoE. For example, in April 2023, a new methodology was produced based on a whole of society approach as a 'dashboard' for policymakers to decide which resources, tools and measures to mobilise at EU, Member State or operational level – it provides a resilience framework against hybrid threats in the EU. This includes mapping how malicious actors use various tools against different domains; helps detect hostile activity and intensity; facilitates the anticipation of damage to democracies; and assesses impacts

[22] This is one key reason for the establishment of the Azure Forum.
[23] https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

of possible hybrid attacks and campaigns.[24] Other examples include the conceptual model (2021) which is described as widely used by policy-makers across Europe.[25] It aims to facilitate the early detection of hybrid threats; the identification of gaps in preparedness; and the development of effective measures to counter malign activities.

[24] https://joint-research-centre.ec.europa.eu/jrc-news/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en

[25] Hybrid threats: a comprehensive resilience ecosystem, 2023.

Annex 1: 'Table 1: Tools of hybrid threat activity', Giannopoulos, G., Smith, H., Theocharidou, M., 'The Landscape of Hybrid Threats: A conceptual model', European Commission, Ispra, 2020, PUBSY No. 123305.

Tool	Affected domains
Physical operations against infrastructure	Infrastructure, Economy, Cyber, Space, Military/Defence, Information, Social/Societal, Public Administration
Creating and exploiting infrastructure dependency (including civil-military dependency)	Infrastructure, Economy, Cyber, Space, Military/Defence, Public Administration
Creating or exploiting economic dependencies	Economy, Diplomacy, Political, Public Administration
Foreign direct investment	Economy, Infrastructure, Cyber, Space, Military/Defence, Public Administration, Intelligence, Information, Political, Legal
Industrial espionage	Economy, Infrastructure, Cyber, Space, Intelligence, Information
Undermining the opponent's national economy	Economy, Public Administration, Political, Diplomacy
Leveraging economic difficulties	Economy, Public Administration, Political, Diplomacy
Cyber espionage	Infrastructure, Space, Cyber, Military/Defence, Public Administration
Cyber operations	Infrastructure, Space, Cyber, Social/Societal, Public Administration, Military/Defence
Airspace violation	Military/Defence, Social/Societal, Political, Diplomacy
Territorial water violation	Military/Defence, Social/Societal, Political, Diplomacy
Weapons proliferation	Military/Defence
Exploiting immigration for political influencing	Political, Social/Societal
Media control and interference	Information, (Media) Infrastructure, Social/Societal, Culture
Disinformation campaigns and propaganda	Social/Societal, Information, Political, Cyber, Culture, Public Administration
Influencing curricula and academia	Social/Societal, Culture
Electronic operations (GNSS jamming and spoofing)	Space, Cyber, Infrastructure, Economy, Military/Defence

Tool	Affected domains
Armed forces conventional/sub-conventional operations	Military/Defence
Paramilitary organizations (proxies)	Military/Defence
Military exercises	Military/Defence, Diplomacy, Political, Societal
Engaging diasporas for influencing	Political, Diplomacy, Social/Societal, Culture, Intelligence, Information
Financing cultural groups and think tanks	Societal, Culture, Political, Diplomacy
Exploitation of sociocultural cleavages (ethnic, religion and culture)	Social/Societal, Culture
Promoting social unrest	Infrastructure, Social/Societal, Economy, Political
Manipulating discourses on migration to polarize societies and undermine liberal democracies	Social/societal, Culture, Political, Legal
Exploiting vulnerabilities in public administration (including emergency management)	Public Administration, Political, Social/Societal
Promoting and exploiting corruption	Public Administration, Economy, Legal, Social/Societal
Exploiting thresholds, non-attribution, gaps and uncertainty in the law	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
Leveraging legal rules, processes, institutions and arguments	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
Intelligence preparation	Intelligence, Military/Defence
Clandestine operations	Intelligence, Military/Defence
Infiltration	Intelligence, Military/Defence
Diplomatic sanctions	Diplomacy, Political, Economy
Boycotts	Diplomacy, Political, Economy
Embassies	Diplomacy, Political, Intelligence, Social/Societal
Creating confusion or a contradictory narrative	Social/Societal, Information, Diplomacy,
Migration as a bargaining chip in international relations	Social/Societal, Diplomacy, Political
Discrediting leadership and/or candidates	Political, Public Administration, Social/Societal
Support of political actors	Political, Public Administration, Social/Societal
Coercion of politicians and/or government	Political, Public Administration, Legal

Annex 2: Extract from 'Maturing national responses to hybrid influencing and cyber threats: A primer on Finland's approach', Azure Forum Strategic Insight, Jarmo Sareva, Ambassador for Cyber Affairs and Liisa Talonpoika, Ambassador for Hybrid Affairs at the Ministry for Foreign Affairs of Finland, 02 March 2022.

Summary
The current geopolitical situation has highlighted the need for a comprehensive response to both cyber and hybrid threats. **Finland's model of comprehensive security also supports our overall resilience against these threats.** The goal is to protect all of society's vital functions through a collaborative approach involving authorities, the private sector, civil society organisations, academia, and private citizens. In this regard, a high educational level, cyber skills, media literacy, social trust and cohesion as well as low corruption are important. Our legal framework further supports this whole of government approach whereby new legislation is adopted as needed to raise preparedness. During the last several years alone, Finland has updated its legislative tools in areas such as intelligence, network security, ownership of real estate, dual nationality and international assistance.

Understanding Finland's approach to hybrid influencing

In the EU, Finland supports the development of a hybrid toolbox as part of the Union's future Strategic Compass. We need a clear set of options for external action to counter hybrid threats as well as a framework to use those options. In this case, the EU Cyber Diplomacy toolbox which already exists is used as a model in developing the hybrid toolbox. To complement national and EU-wide cooperation, wider international engagement is also important, and is actively used, including through Nordic, bilateral and NATO cooperation.

Several actors must be involved due to the complex nature of hybrid threats, especially since the necessary tasks can only be performed through cooperation and there is no 'one size fits all' solution. In Finland's case, the following actors are involved:

- Given the **Ministry of Foreign Affairs'** focus on contributing to national activities and especially at international fora, it has, for a number of years, had Cyber and Hybrid Ambassadors in its technology and security team, alongside a senior expert on strategic communications advising the East department.
- The **EU-secretariat in the Prime Minister's office** coordinates EU positions and its press department has a team dealing with strategic communications, media awareness and media reading skills. The Government's 24/7 situation centre produces material, both on a daily basis as well as larger analyses. The Prime Minister's office also works closely with the office of the President.
- The **Government's Security Committee**, which has its own secretariat, consists of permanent secretaries of all ministries and director generals of relevant authorities. It also produces the security strategy for society, which is updated every three to four years with a new version due to be released soon.
- **Heads of Preparedness from ministries and relevant authorities meet regularly.**
- The **Department for Democracy and Public Law of the Ministry of Justice** oversees elections, election security and leads the work to combat election interference. A civil servant level coordination group deals with elections and a special webpage provides information to voters.

- The **Ministry of Interior's Unit for National Security, Ministry of Defense, Defense Command and Security and Intelligence Service** are vital actors in safeguarding Finland's security across all dimensions of hybrid threats in their field of expertise. Coordination is achieved through existing structures or on an ad hoc basis, depending on the hybrid domain in question. **Almost all other ministries are also involved**, due to the complex nature of hybrid influencing. Some examples of these Ministries include the Ministry of Communications (for cyber and network technologies), Ministry of Economic Affairs (for energy, regional actors and space), and the Ministry of Education and Culture (for universities and research). The Parliament and its committees deal with hybrid-related questions regularly, while the embassy network is involved in producing material that can feed into domestic endeavours.
- Other key authorities, all closely linked to respective Ministries, which deal with hybrid questions include the **National Emergency Supply Agency; Finnish Institute for Health and Welfare; Digital and Population Data Service; and National Cybersecurity Centre**.
- **Finland's National Defense College** organises courses at the national and local level, based on a whole of government approach to security. The private sector, Parliament, NGOs, media outlets, Government officials and various authorities are all involved in this work, culminating in over 10,000 leaders from all walks of life having completed three-week training on how to protect society during a crisis.
- Finland also participates actively in the **European Centre of Excellence for Countering Hybrid Threats** (Hybrid CoE) located in Helsinki. The centre brings added value through research, awareness raising, sharing best practices and exercises. Finland also participates in other relevant Centres of Excellence, namely the **NATO Cooperative Cyber Defence Centre of Excellence** in Tallinn and the **NATO Strategic Communications Centre of Excellence** in Riga.

In short, it is essential to be one step ahead and prepared, focusing on what might happen next, instead of being reactive to events. While this is not easy, **foresight** planning can be successfully carried out if signs can be detected. Monitoring of evolving trends in the operating environment and reviewing possible scenarios helps to prepare for the unexpected.

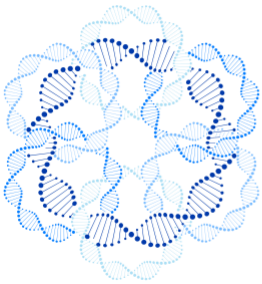
Annex 3: Examples of lessons from recent crisis communications in the Irish context

The Covid-19 crisis in Ireland acted as a forcing function to establish effective crisis communications, sparking a realisation of the importance of such crisis communications and especially in relation to misinformation/disinformation. The subsequent criminal ransomware cyber attack against the HSE further reiterated the importance of crisis communications.

Challenges in the Irish context might include, for example, an historical or cultural legacy of lack of citizens' trust in governmental communications – sometimes criticised as government propaganda. Should this be the case, awareness-raising activities might also be relevant, including exploring the importance of 'trust' in this context of building resilience.

[26]For example, the case study of the Covid crisis indicated to some Irish experts that there was an important role for independent and safe voices such as academics where there was nothing for them to gain so to speak. These voices became sources of reliable information. Notably, it is also beginning to become clear among some Irish experts that fact-checking/fact-checking organisations are not enough in the wake of domestic lessons learned during the Covid-19 crisis.

[26] Author observations, IUSA event, Dublin, 2022.



THE AZURE FORUM
FOR CONTEMPORARY SECURITY STRATEGY

The Azure Forum for Contemporary Security Strategy is Ireland's first and only independent think tank dedicated to providing recommendations on peace, security and defence. As Ireland's first national security research institute, the Forum aims to contribute to national and international security analysis and strategic studies for a more peaceful, secure, resilient and prosperous future nationally and globally at a time of emerging global risk.