NATO Strategic Communications Centre of Excellence | BRIEF

27th November 2021

INFORMATION INFLUENCE[1] AS A TOOL OF HYBRID THREATS

1. Since the end of the Cold War, liberal democracies of the Western world have been increasingly challenged by autocracies, whose leaders feel endangered by universal freedoms, which they believe, will lead to a loss of control and political power. To minimise the pernicious influence of the liberal world, authoritarian regimes are questioning success stories of democracies by sowing seeds of distrust into the minds of people and applying **wide range of hybrid tools in their aggressive and cynical manipulations**.

2. By their very nature, hybrid threats are adaptive and often difficult to detect, identify and attribute. Authoritarian states employ creative means and ways to subvert the established rules of the international system, exploiting vulnerabilities within their targeted nation. **The areas of concern are most likely not obvious today but yet to emerge**. Despite the challenge of predictability, there are identifiable characteristics and patterns regarding information influence, which can be used to support horizon scanning and threat analysis.

3. Advances in **technology have supercharged the opportunities** available to actors wishing to polarise societies, cause discord amongst different identity groups and influence legitimate political discourse. These activities, referred to as 'information influencing', 'hostile information activities', 'information operations'[2] or 'hybrid influencing'[3] are intentionally harmful, deceptive and disruptive. They exploit the open nature of democratic societies to deliberately interfere in internal affairs and create a climate of distrust.

4. Levers of influence commonly used in the information space by hostile actors tend to relate to dissemination channels such as **media organisations and social media platforms**, or the intangible expression of soft power and cultural influence through education or outreach programmes. These can include **political statements, diplomacy, and control of the media, hack-and-leak operations**, and a whole range of methods involving **online platforms.** Disinformation remains a significant challenge such as hard to verify content, cross-platform sharing of malicious material, closed groups and online communities, harmful algorithms, information laundering and encryption.[4]

[1] Activities conducted by foreign powers to influence the perceptions, behaviour and decisions of target groups to the benefit of foreign powers. https://portal.research.lu.se/en/publications/countering-information-influence-activities-the-state-of-the-art

[2] "actions taken by organized actors (governments or non-state actors) **to distort domestic or foreign political sentiment**, most frequently to achieve a strategic and/or geopolitical outcome." https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

[3] According to the European Centre for Countering Hybrid Threats " Influencing is part of traditional state policies and most states try to influence in the international politics. However, there are two kind of influencing, the one that is more open with clear goals – conventional influencing – and then there is influencing that is part of the Hybrid Threats – often referred to as Hybrid Influencing. https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

[4] https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf

5. StratCom COE research indicates that the most popular narrative strategy used by illiberal countries is to **create a threat** to which they believe they are justified to respond. This can be combined with narratives of **blaming or discrediting** others, and **playing the victim**. Narratives tend to follow themes: international order and ethics; governance and human rights; identity and culture; economics; defence and security.[5]

6. In recent months, the StratCom COE has seen an increase of **malign activities** in the Transatlantic information space attributable to **Russia and China**, as well as the emergence of Belarus as an active source disinformation in the region. Such activities target different layers of societies and a diversity of audiences simultaneously.

7. By all accepted definitions, events orchestrated by the Minsk regime on the EU borders of Poland, Latvia and Lithuania constitute a hybrid threat**. Belarus is employing a range of instruments: international law; the use of force; tourist visa issuance and the leveraging of energy supply, to further their strategic aims.** They are amplified and reinforced by activities in the information space enabled by a de facto state monopoly – including **ownership of mainstream media, regulation of the internet and intimidation of journalists** - providing near total control over information about political, social, and economic affairs. The Belarusian government has been linked to campaigns of hacking and disinformation, aimed at the regime's critics including NATO and foreign governments.[6]

8. **No organisation or state has the capacity to tackle such threats alone.** Effective responses demand a blend of military and non-military means and constructive cooperation between governments and academia, industry and civil society. Persistent preparation, involving the whole-of-government and allowing the formulation of threats, risks and vulnerabilities to critical functions, is essential. This means **training, education and exercises**. Governments need a toolkit of capabilities ready to compete against hostile states in order to prevent and counter those threats. This preparation contributes significantly to **societal resilience and deterrence**.

9. **Hybrid threats, which exploit the information environment, are highly adaptive and opportunistic; therefore, they need to be detected and identified before they risk escalating into something more sinister**. Monitoring and understanding the information environment, with timely identification of hostile **measures** as they develop and the **narratives** that accompany them, remain a top priority. This increases the opportunity for targeted nations to get ahead of the curve and establish the facts of the matter in public discourse. It also makes available **credible and compelling evidence to support attribution**.

10. Certain scenarios are anticipated and already considered in the calculus of respective governments. But unexpected threats, with the potential for disproportionately unfavourable outcomes, can emerge from across the continuum of peace, crisis and war.

[5] https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213 p12.
[6] https://news.sky.com/story/belarusian-military-linked-to-hacking-and-disinformation-campaigns-targeting-regime-critics-12469385